THE UNIVERSITY OF ALBERTA

ON THE DENSITY OF SETS OF INTEGERS

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS

by

HARVEY LESLIE ABBOTT

EDMONTON, ALBERTA

February, 1963

ABSTRACT

This thesis deals with some problems in additive number theory. The first two chapters are concerned with the addition of two or more sets of positive integers and contain an exposition of some relationships between the density of the sum set and the densities of the various summands. In the last chapter some results concerning the number of solutions of $n = a_i + a_j$, where the a's are members of some sequence of positive integers, are discussed.

ACKNOWLEDGEMENTS

The writer would like to thank Dr. Leo Moser for his guidance and advice.

TABLE OF CONTENTS

	Page
CHAPTER I - SCHNIRELMANN DENSITY AND RELATED TOPICS	
1. The $\alpha + \beta$ Theorem	1
2. Some Best Possible Results	13
3. Generalization of the $\alpha + \beta$ Theorem	17
4. Essential Components	27
5. Modified Schnirelmann Densities	31
6. Some Additional Results	37
CHAPTER II - ASYMPTOTIC DENSITY AND RELATED TOPICS	
1. Introduction.	41
2. The Analogue of the $\alpha + \beta$ Theorem	41
3. Complementary Sets of Positive Integers	44
4. Hanani's Conjecture	54
5. Some Results of Moser on the Addition of Two Sets of Integers.	60
CHAPTER III - SOME RELATED TOPICS	
1. A Theorem of Erdös and Fuchs	70
BIBLIOGRAPHY	87

CHAPTER I

SCHNIRELMANN DENSITY AND RELATED TOPICS

1. The $\alpha + \beta$ Theorem

We begin with some remarks on notation. Throughout this thesis, unless otherwise stated, capital Latin letters, with or without affixes, denote sets of distinct positive integers. J denotes the set of all positive integers and V is the empty set. By the sum of m sets, A_1, $A_2, \ldots, A_m$, not necessarily distinct, is meant the set C of all distinct positive integers of the form $e_1a_1 + e_2a_2 + \ldots + e_ma_m$, where $a_i \in A_i$ and $e_i = 0$ or 1, $i = 1, 2, \ldots, m$. Note that for at least one j we must have $e_j = 1$. We write $C = A_1 + A_2 + \ldots + A_m$. We shall be concerned largely with the sum of two sets in which case, on setting $A_1 = A$ and $A_2 = B$, we have $C = \{a, b, a + b;\ a \in A, b \in B\}$. If n is an integer, by $A(n)$ we mean the number of positive integers in A which do not exceed n. If $a \in A$, $a + \ell + 1 \in A$ and $a + i \notin A$ for $i = 1, 2, \ldots, \ell$, then the set $\{a + i;\ i = 1, 2, \ldots, \ell\}$ is called a gap of length ℓ.

The Schnirelmann density, $d(A)$, of a set A is defined as follows:

(1.1.1) $$d(A) = \underset{n \geq 1}{\text{g.l.b.}} \frac{A(n)}{n} .$$

This implies that $A(n) \geq d(A)n$ for all $n \geq 1$ and if $A(n) \geq \theta n$ for all $n \geq 1$, then $d(A) \geq \theta$. The following statements are obvious:

(1.1.2) $$0 \leq d(A) \leq 1$$

(1.1.3) If $1 \notin A$, then $d(A) = 0$

(1.1.4) $d(A) = 1$ if, and only if, $A = J$.

Let $d(A) = \alpha$, $d(B) = \beta$ and $d(C) = d(A + B) = \gamma$. We wish to establish some inequalities involving α , β and γ .

<u>Theorem 1.1.1</u> $\gamma \geq \alpha + \beta - \alpha\beta$.

<u>Proof</u>: If $\alpha = 1$ the theorem is obviously true since then $\alpha + \beta - \alpha\beta = 1$ and $\gamma = 1$. Hence we may assume that there are gaps in A. Let n be a positive integer. Let there be m gaps of length $\ell_1, \ell_2, \ldots, \ell_m$ in A among the integers which do not exceed n. Let $n - \ell_{m+1}$ be the largest integer in A not exceeding n; $0 \leq \ell_{m+1} \leq n - 1$. (We are assuming that $1 \in A$ since otherwise $\alpha = 0$ and the theorem is trivial.) Then

$$(1.1.5) \qquad n - A(n) = \ell_1 + \ell_2 + \ldots + \ell_m + \ell_{m+1} .$$

For $i = 1, 2, \ldots, m$ let the gap of length ℓ_i be defined by $a_i \in A$, $a_i + \ell_i + 1 \in A$, $a_i + \nu \notin A$, $\nu = 1, 2, \ldots, \ell_i$. Add the $B(\ell_i)$ integers of B which do not exceed ℓ_i to a_i. This yields $B(\ell_i)$ integers in A + B between a_i and $a_i + \ell_i + 1$. Add the $B(\ell_{m+1})$ integers of B not exceeding ℓ_{m+1} to $n - \ell_{m+1}$ to get $B(\ell_{m+1})$ integers in A + B between $n - \ell_{m+1}$ and n. Then we have

$$(1.1.6) \qquad \begin{aligned} C(n) &\geq A(n) + B(\ell_1) + B(\ell_2) + \ldots + B(\ell_m) + B(\ell_{m+1}) \\ &\geq A(n) + \beta(\ell_1 + \ell_2 + \ldots + \ell_m + \ell_{m+1}) \\ &= A(n) + \beta(n - A(n)) , \quad \text{by (1.1.5)} \\ &= A(n)\,[1 - \beta] + \beta n \\ &\geq \alpha(1 - \beta)\, n + \beta n \\ &= (\alpha + \beta - \alpha\beta)\, n . \end{aligned}$$

Since n is arbitrary, (1.1.6) is true for all n. Hence $\gamma \geq \alpha + \beta - \alpha\beta$. We may write the result as

$$(1.1.7) \qquad 1 - d(A + B) \leq (1 - d(A))(1 - d(B))$$

in which form it may be easily generalized by induction to

$$(1.1.8) \qquad 1 - d(A_1 + A_2 + \dots + A_k) \leq \prod_{i=1}^{k} (1 - d(A_i)).$$

Theorem 1.1.1 was proved by Landau [23] and Schnirelmann [39]. It was conjectured by Khinchin [22] that the following sharper result holds: if $\alpha + \beta \leq 1$, then $\gamma \geq \alpha + \beta$ and if $\alpha + \beta > 1$, then $\gamma = 1$. Khinchin [22] was able to prove this for the cases $\alpha = \beta$ and $\alpha = 1 - 2\beta$. Various other partial results were obtained by Brauer [4] and Schur [40] but the so-called $\alpha + \beta$ theorem refused to yield to the attacks of many great scholars. A proof of the theorem was finally given by H. B. Mann [28] in 1942. His proof, although elementary, was difficult. A somewhat simpler proof was given by Artin and Scherk [1] in 1943. Before discussing proofs of the $\alpha + \beta$ theorem we return again to Theorem 1.1.1 and discuss some important consequences. We shall need the following lemma.

<u>Lemma 1.1.1</u> Let n be a positive integer. If $A(n) + B(n) \geq n$, then $n \in A + B = C$.

<u>Proof</u>: We have $a_1 < a_2 < \dots < a_{A(n)} \leq n$ and $b_1 < b_2 < \dots < b_{B(n)} \leq n$. If $a_{A(n)} = n$ or $b_{B(n)} = n$, we have finished. Hence we may assume $a_{A(n)} < n$ and $b_{B(n)} < n$. The $A(n) + B(n)$ numbers $n - b_1, n - b_2, \dots, n - b_{B(n)}, a_1, a_2, \dots, a_{A(n)}$ are all less than n and since $A(n) + B(n) \geq n$, these numbers cannot all be distinct. Hence for some i and j, where $1 \leq i \leq A(n)$, $1 \leq j \leq B(n)$, we must have $a_i = n - b_j$.

This implies that $n \in C$.

A set A is said to form a basis of order h, where h is a positive integer, if every positive integer is the sum of at most h elements of A. This is equivalent to saying that A is a basis of order h if $J = A + A + \ldots + A$, where there are h summands. We prove the following theorem.

<u>Theorem 1.1.2</u> Let $d(A) = \alpha > 0$. Then A is a basis.

<u>Proof</u>: Let A_k be the sum of k sets each of which is identical with A. Then, by (1.1.8)

$$1 - d(A_k) \leq (1 - \alpha)^k$$

so that

$$d(A_k) \geq 1 - (1 - \alpha)^k.$$

For k sufficiently large $(1 - \alpha)^k \leq 1/2$ and hence $d(A_k) \geq 1/2$. It follows that $A_k(n) \geq 1/2\ n$, for every n, and hence that $A_k(n) + A_k(n) \geq n$, for every n. By Lemma 1.1.1, $n \in A_k + A_k = A_{2k}$, which implies that $A_{2k} = J$, i.e. A is a basis.

Let P be the set consisting of 1 and all primes. It is clear from Chebychev's theorem that $d(P) = 0$. However, Schnirelmann [39] was able to show that $d(P + P) > 0$. By Theorem 1.1.2, P + P, and hence P, is a basis.

We return to the $\alpha + \beta$ theorem. We may assume without loss of generality that $1 \in A$ and $1 \in B$, since otherwise the theorem is trivial. The proof of the theorem depends upon the following

<u>Fundamental Lemma</u> Let n be a positive integer. Then there exists a positive integer m satisfying $1 \leq m \leq n$ such that $C(n) - C(n - m) \geq (\alpha + \beta) m$; $\alpha + \beta \leq 1$.

Suppose $n \in C$. We may then choose $m = 1$, since $C(n) - C(n - 1) = 1 \geq (\alpha + \beta)1$. Henceforth we assume that $n \notin C$.

Let c and c' be arbitrary numbers of the segment $[1, n]$ which do not appear in C. C is said to be <u>normal</u> if, for every such pair c, c', the relations $c + c' - n \notin C$, and $c + c' - n \neq 0$ hold. The case where $c = c'$ is not excluded.

<u>Proof of the Fundamental Lemma when C is normal</u>

Let m be the smallest integer which does not occur in C. Since $n \notin C$, $m \leq n$ and since $1 \in C$, $m \geq 2$. Let s be an arbitrary positive integer such that $n - m < s < n$. Then $0 < s + m - n < m$. We assert that $s \in C$. To see this suppose that $s \notin C$. Then, since $m \notin C$, $s + m - n \notin C$, as C is normal. This contradicts the fact that m is the smallest positive integer not occuring in C. Hence $s \in C$. It follows that <u>all</u> numbers s such that $n - m < s < n$ are in C. There are $m - 1$ such numbers. Hence $C(n) - C(n - m) = m - 1$. Since $m \notin C$, we must have $A(m) + B(m) \leq m - 1$, by Lemma 1.1.1. Hence $C(n) - C(n - m) = m - 1 \geq A(m) + B(m) \geq (\alpha + \beta)m$. The fundamental lemma is therefore valid for normal sequences. Henceforth we assume that C is not normal.

<u>Proof of the Fundamental Lemma when C is not normal</u>.

The proof in this case is considerably more complicated. The idea of the proof is as follows. We construct sets B' and C' such that

$B' \supset B$, $C' \supset C$, $C' = A + B'$ and C' is normal. It will then follow that $C'(n) - C'(n - m) \geq A(m) + B'(m)$, where m is the smallest positive integer not occurring in C'. C' and B' are to be constructed in such a manner that $C'(n) - C'(n - m) \geq A(m) + B'(m)$ implies $C(n) - C(n - m) \geq A(m) + B(m)$. The fundamental lemma will then follow. We proceed with the details of the proof.

Since C is not normal, there exist at least two positive integers c and c' (these may not be distinct) in the segment $[1, n]$ such that $c \notin C$, $c' \notin C$, and $c + c' - n \in C$ or $c + c' - n = 0$. Since $n \notin C$, we must have $c' < n$, $c < n$. Since $C = A + B$, we have

$$(1.1.9) \qquad c + c' - n = a + b$$

where $a \in A$ or $a = 0$, $b \in B$ or $b = 0$, $a \leq n$, $b \leq n$. Let β_o be the smallest $b \in B$ (or $\beta_o = 0$) for which the equation

$$(1.1.10) \qquad c + c' - n = a + \beta_o$$

has solutions c, c', a satisfying $c \notin C$, $c' \notin C$, $a \in A$ or $a = 0$, $c < n$, $c' < n$, $a \leq n$.

Let C^* be the set of all c and c' satisfying (1.1.10) and the added conditions. It is clear that all numbers in C^* are in the segment $[1, n]$ and that $C \cap C^* = V$. Put $C_1 = C \cup C^*$ and call C_1 the canonical extension of C.

Let $B^* = \{\beta_o + n - c;\ c \in C^*\}$. If $b^* \in B^*$, then for some $c \in C^*$ and $a \in A$ or $a = 0$, we have $b^* = c - a \leq c < n$. Also $b^* = \beta_o + n - c > \beta_o \geq 0$ so that all numbers in B^* are in the segment $[1, n]$. It is easy to

see that $B \cap B^* = V$. We put $B_1 = B \cup B^*$ and call B_1 the canonical extension of B. Also, call β_o the basis of the canonical extensions of B and C.

<u>Lemma 1.1.2</u> $\quad A + B_1 = C_1$

<u>Proof</u>: We show first that $A + B_1 \subset C_1$. Now $A + B_1 = \{a, b_1, a + b_1;\ a \in A, b_1 \in B_1\}$. We clearly have $a \in A \subset C \subset C_1$. Let $b_1 \in B_1$ and let $a \in A$ or $a = 0$. If $b_1 \in B$, then $a + b_1 \in A + B = C \subset C_1$. If $b_1 \in B^*$ either $a + b_1 \in C \subset C_1$ or $a + b_1 \notin C$. Suppose the latter occurs. By the definition of B^*, we have $b_1 = \beta_o + n - c$ where $c \in C$. Hence $(a + b_1) + c - n = a + \beta_o$. By the definition of C^*, we have $a + b_1 \in C^* \subset C_1$. Hence $A + B_1 \subset C_1$.

Secondly we show that $C_1 \subset A + B_1$. Let $c \in C_1$. Then, either $c \in C = A + B \subset A + B_1$ or $c \in C^*$. If the latter is so, then for some $a \in A$ or $a = 0$, the number $b^* = c - a$ occurs in B^*. Hence $c = a + b^* \in A + B^* \subset A + B_1$. It follows that $C_1 \subset A + B_1$ and hence that $C_1 = A + B_1$.

<u>Lemma 1.1.3</u> $\quad n \notin C_1$

<u>Proof</u>: Assume that $n \in C_1 = C \cup C^*$. Since $C \cap C^* = V$ and since $n \notin C$ we must have $n \in C^*$. This is impossible as all numbers in C^* are less than n. The lemma follows.

If C_1 is not normal, then by Lemmas 1.1.2 and 1.1.3 the sets A, B_1, C_1 have all the properties of A, B, C which are necessary to form new canonical extensions. We choose a new basis β_1, define the sets B_1^*, C_1^* as before, and put $B_1 \cup B_1^* = B_2$, $C_1 \cup C_1^* = C_2$. We may assert $A + B_2 = C_2$, $n \notin C_2$. This process can be repeated until one of the

extensions, C_h, is normal. This must occur at some stage since in every extension we add new numbers from the segment [1, n] to the sets B_μ, C_μ to get the sets $B_{\mu+1}$, $C_{\mu+1}$. There must be a stage at which we can add no new numbers. The sets at which we arrive then are normal. We get therefore two finite sequences of sets

$$B = B_o \subset B_1 \subset B_2 \subset \ldots \subset B_h$$
$$C = C_o \subset C_1 \subset C_2 \subset \ldots \subset C_h$$

where $B_{\mu+1}$ (respectively $C_{\mu+1}$) contains numbers not in B_μ (respectively C_μ). These numbers make up the sets $B_\mu{}^*$ (respectively $C_\mu{}^*$) so that $B_{\mu+1} = B_\mu \cup B_\mu{}^*$ and $C_{\mu+1} = C_\mu \cup C_\mu{}^*$ for $0 \leq \mu \leq h - 1$. Denote by β_μ the basis of the extension from B_μ and C_μ to $B_{\mu+1}$ and $C_{\mu+1}$. We have $A + B_\mu = C_\mu$ and $n \notin C_\mu$ for $0 \leq \mu \leq h$. The set C_h is normal but the sets C_μ, for $0 \leq \mu \leq h - 1$, are not. We have put $B = B_o$ and $C = C_o$.

<u>Lemma 1.1.4</u> $\beta_\mu > \beta_{\mu-1}$, $1 \leq \mu \leq h - 1$.

<u>Proof</u>: It is sufficient to show $\beta_1 > \beta_o$. There are two cases to be considered.

<u>Case 1</u>. $\beta_o = 0$.

Suppose that $\beta_1 = 0$. There exist integers $a \in A$, or $a = 0$, $c_1 \notin C_1$ $c_1' \notin C_1$ such that $c_1 + c_1' - n = a + \beta_1 = a + \beta_o$. This implies $c_1 \in C^*$ and $c_1' \in C^*$. Since $C_1 = C \cup C^*$, we have a contradiction. Hence $\beta_1 > \beta_o$.

<u>Case 2</u>. $\beta_o \in B$.

There exist integers $a \in A$ or $a = 0$, $c_1 \notin C_1$, $c_1' \notin C_1$ such that $c_1 + c_1' - n = a + \beta_1$, where either $\beta_1 = 0$ or $\beta_1 \in B_1$. Clearly,

$\beta_1 = 0$ implies that we should have $\beta_o = 0$ which is not the case. If $\beta_1 \in B_1$, then either $\beta_1 \in B^*$ or $\beta_1 \in B$. If $\beta_1 \in B^*$, then $\beta_1 = \beta_o + n - c$ where $c \in C^*$ and $c < n$. It follows that $\beta_1 > \beta_o$. Let $\beta_1 \in B$. For suitable $c_1 \notin C_1$, $c_1' \notin C_1$, $a \in A$ or $a = 0$ we have $c_1 + c_1' - n = a + \beta_1 \in A + B = C$. Now $\beta_1 \geq \beta_o$ by the minimal property of β_o. Suppose $\beta_1 = \beta_o$. Then $c_1 \in C^* \subset C_1$ and $c_1' \in C^* \subset C_1$ which is not the case. Hence $\beta_1 > \beta_o$.

In what follows let m be the smallest positive integer which does not appear in C_h.

<u>Lemma 1.1.5</u> If $c \in C_\mu^*$, $0 \leq \mu \leq h - 1$ and if $n - m < c < n$ then $n - m + \beta_\mu < c < n$.

<u>Proof</u>: From $n - m < c < n$ it follows that $0 < m + c - n < m$. Since m is the smallest positive integer not in C_h, $m + c - n \in C_h$. We have $C_h = C_\mu \cup C_\mu^* \cup C^*_{\mu+1} \cup \dots \cup C^*_{h-1}$. The sets in this union are disjoint. We consider two cases.

<u>Case 1.</u> $m + c - n \in C_\mu = A + B_\mu$.

We have $m + c - n = a + b_\mu$ where $a \in A$ or $a = 0$, and $b_\mu \in B_\mu$ or $b_\mu = 0$. Now $m \notin C_\mu$ and $c \notin C_\mu$. By the minimal property of β_μ we have $b_\mu \geq \beta_\mu$. $b_\mu = \beta_\mu$ cannot hold since if it did we would have $m \in C_\mu^* \subset C_{\mu+1} \subset C_h$ and this is not the case. Hence $b_\mu > \beta_\mu$. This implies that $c > n - m + \beta_\mu$.

<u>Case 2</u>. $m + c - n \in C_\nu^*$ where $\mu \leq \nu \leq h - 1$.

By definition of C_ν^*, for some $a \in A$ or $a = 0$ and $c' \in C_\nu^*$, we have $(m + c - n) + c' - n = a + \beta_\nu$. Hence $(m + c - n) \geq (m + c - n) - a = \beta_\nu + n - c' > \beta_\nu \geq \beta_\mu$. Hence $c > n - m + \beta_\mu$ and the lemma follows.

<u>Lemma 1.1.6</u> $C_\mu{*}(n) - C_\mu{*}(n-m) = B_\mu{*}(m)$ for $\mu = 0, 1, \ldots, h-1$

<u>Proof</u>: It is easy to check that if b and c are related by the formula $b = \beta_\mu + n - c$, then $b \in B_\mu{*}$ implies $c \in C_\mu{*}$ and conversely. It is also readily verified that $n - m + \beta_\mu < c < n$ implies $\beta_\mu < b < m$ and conversely. Hence we have

$$(1.1.11) \qquad C_\mu{*}(n) - C_\mu{*}(n - m + \beta_\mu) = B_\mu{*}(m) - B_\mu{*}(\beta_\mu)$$

By Lemma 1.1.5, $C_\mu{*}(n - m + \beta_\mu) = C_\mu{*}(n-m)$. It is also clear that $B_\mu{*}(\beta_\mu) = 0$. This with (1.1.11) yields

$$C_\mu{*}(n) - C_\mu{*}(n-m) = B_\mu{*}(m),$$

as asserted.

We now have sufficient information about the canonical extensions to enable us to complete the proof of the fundamental lemma. Since C_h is normal and $C_h = A + B_h$ we have

$$(1.1.12) \qquad C_h(n) - C_h(n-m) \geq A(m) + B_h(m)$$

Now

$$C_h = C \cup C_o{*} \cup C_1{*} \cup C_2{*} \cup \ldots \cup C^*_{h-1}$$

and

$$B_h = B \cup B_o{*} \cup B_1{*} \cup B_2{*} \cup \ldots \cup B^*_{h-1}$$

The sets appearing in any one of these two unions are disjoint. Hence

$$(1.1.13) \quad C_h(n) - C_h(n-m) = C(n) - C(n-m) + \sum_{\mu=0}^{h-1} [C_\mu{*}(n) - C_\mu{*}(n-m)]$$

$$(1.1.14) \qquad B_h(m) = B(m) + \sum_{\mu=0}^{h-1} B_\mu{*}(m) .$$

From (1.1.12), (1.1.13), (1.1.14) and Lemma 1.1.6 we have

$$C(n) - C(n - m) \geq A(m) + B(m) \geq (\alpha + \beta)m.$$

The fundamental lemma is therefore established.

Proof of the $\alpha + \beta$ Theorem

We have to show that if $d(A) = \alpha$, $d(B) = \beta$, $d(C) = d(A + B) = \gamma$ then (i) $\gamma \geq \alpha + \beta$ if $\alpha + \beta \leq 1$

(ii) $\gamma = 1$ if $\alpha + \beta > 1$.

(i) By the average density of the set C in the segment [r, s] we mean $\dfrac{C(s) - C(r-1)}{s - r + 1}$. The fundamental lemma now states that there exists a remainder [n - m + 1, n] of the segment [1, n] in which the average density is at least $\alpha + \beta$. Similarly there exists a remainder [n - m - m' + 1, n - m] of the segment [1, n - m] in which the average density of C is at least $\alpha + \beta$. By continuing in this fashion, the segment [1, n] is divided into a finite number of such segments in each of which the average density of C is at least $\alpha + \beta$. Hence the average density of C in [1, n] is at least $\alpha + \beta$, i.e. $\dfrac{C(n)}{n} \geq \alpha + \beta$. Since n is arbitrary, $C(n) \geq (\alpha + \beta)n$ for all n. Hence $\gamma \geq \alpha + \beta$.

(ii) Let $\alpha + \beta > 1$. We need to show that C = A + B = J. Suppose $n \notin C$ and let $a_1, a_2, \ldots, a_{A(n)}$ be the integers in A which do not exceed n. Then the integers, $n, n - a_1, n - a_2, \ldots, n - a_{A(n)}$ are not in B. Hence β is at most $1 - \dfrac{A(n) + 1}{n}$. Also $\alpha \leq \dfrac{A(n)}{n}$ so that $\alpha + \beta \leq \dfrac{A(n)}{n} + 1 - \dfrac{A(n)+1}{n} = 1 - \dfrac{1}{n} < 1$, which is false. Hence $n \in C$. Hence $C = J$ and $\gamma = 1$.

The above theorem can easily be generalized by induction to the following.

Theorem 1.1.3

Let $d(A_1) = \alpha_1$, $d(A_2) = \alpha_2$, ... , $d(A_k) = \alpha_k$. If $C = A_1 + A_2 + \ldots + A_k$ and $\alpha_1 + \alpha_2 + \ldots + \alpha_k \leq 1$, then $d(C) \geq \alpha_1 + \alpha_2 + \ldots + \alpha_k$. If $\alpha_1 + \alpha_2 + \ldots + \alpha_k > 1$, then $d(C) = 1$.

That the $\alpha + \beta$ theorem cannot in general be improved is shown by the following example.

Let $A = B = \{1, 8n;\ n = 1, 2, 3, \ldots\}$. Then $d(A) = d(B) = 1/8$. Also $C = A + B = \{1, 2, 8n, 8n + 1;\ n = 1, 2, 3, \ldots\}$ and $d(C) = 1/4 = d(A) + d(B)$.

It is interesting to note that the preceding proof of the $\alpha + \beta$ theorem can be modified to give the following stronger result. For fixed integral $x \geq 1$, define

$$\alpha(x) = \underset{1 \leq n \leq x}{\text{g.l.b.}} \frac{A(n)}{n} .$$

Define $\beta(x)$ and $\gamma(x)$ in the same way for the sets B and C. Then it is clear from the above proof that if $\alpha(x) + \beta(x) < 1$, then $\gamma(x) \geq \alpha(x) + \beta(x)$ and if $\alpha(x) + \beta(x) \geq 1$, then $\gamma(x) = 1$.

The proof that we have just presented is essentially due to Artin and Scherk [1]. It also appears in a book by A. Y. Khinchin [21].

2. Some Best Possible Results

In this section we discuss the following question. Given real numbers α, β and γ satisfying $\alpha \geq 0$, $\beta \geq 0$ and $\alpha + \beta \leq \gamma \leq 1$, can one find sets A and B such that $d(A) = \alpha$, $d(B) = \beta$ and $d(A + B) = \gamma$. Lepson [25] answered this question in the affirmative for the special case $\gamma = \alpha + \beta$, and the question was settled completely by Cheo [6]. Here we exhibit a construction which is more general than that of Cheo but our proof is essentially the same as his.

Theorem 1.2.1 Let $\alpha \geq 0$, $\beta \geq 0$, $1 \geq \gamma \geq \alpha + \beta$. Then there exist sets A and B such that $d(A) = \alpha$, $d(B) = \beta$ and $d(C) = d(A + B) = \gamma$.

Proof: Let f be a function with the following properties

(i) f is defined on the set of positive integers and assumes positive integral values

(ii) f is monotone increasing

(iii) $f(1) = 1$

(iv) $\lim_{n \to \infty} \frac{f(n)}{f(n+1)} = 0$.

Let $\gamma - \alpha = \delta$ and $\gamma - \beta = \theta$. Then $\delta \geq \beta$ and $\theta \geq \alpha$. For $n \geq 1$ define integers a_n and b_n such that, when n is even,

$$(1.2.1) \begin{cases} \alpha f(n+1) - \alpha f(n) \leq a_n < \alpha f(n+1) - \alpha f(n) + 1 \\ \delta f(n+1) - \delta f(n) \leq b_n < \delta f(n+1) - \delta f(n) + 1, \end{cases}$$

and such that, when n is odd,

$$(1.2.2) \begin{cases} \theta f(n+1) - \theta f(n) \leq a_n < \theta f(n+1) - \theta f(n) + 1 \\ \beta f(n+1) - \beta f(n) \leq b_n < \beta f(n+1) - \beta f(n) + 1. \end{cases}$$

Since $\alpha \leq \theta \leq 1$ and since $\beta \leq \delta \leq 1$, we have for all n

$$(1.2.3) \quad \begin{cases} \alpha f(n+1) - \alpha f(n) \leq a_n \leq f(n+1) - f(n) \\ \beta f(n+1) - \beta f(n) \leq b_n \leq f(n+1) - f(n) . \end{cases}$$

From (1.2.1) and (1.2.2) we have for all n

$$(1.2.4) \quad \gamma f(n+1) - \gamma f(n) \leq a_n + b_n < \gamma f(n+1) - \gamma f(n) + 2 .$$

If n is even we have, by (1.2.1),

$$(1.2.5) \quad \alpha - \alpha \frac{f(n)}{f(n+1)} \leq \frac{a_n}{f(n+1)} < \alpha - \frac{\alpha f(n)}{f(n+1)} + \frac{1}{f(n+1)}$$

For all n, by (1.2.3), we have

$$(1.2.6) \quad \alpha - \frac{\alpha f(n)}{f(n+1)} \leq \frac{a_n}{f(n+1)} \leq 1 - \frac{f(n)}{f(n+1)}$$

From (1.2.5) and (1.2.6) it follows that

$$(1.2.7) \quad \liminf_{n \to \infty} \frac{a_n}{f(n+1)} = \alpha .$$

We define the sets A and B in the following manner.

$$(1.2.8) \quad A = \{1\} \cup \bigcup_{n=1}^{\infty} \{f(n)+1, f(n)+2, \ldots , f(n)+a_n\}$$

$$(1.2.9) \quad B = \{1\} \cup \bigcup_{n=1}^{\infty} \{f(n)+1, f(n)+2, \ldots , f(n)+b_n\}$$

From (1.2.3) and (1.2.8) it is clear that $f(n-1) + a_{n-1}$ and $f(n) + 1$ are consecutive elements of A. Now $f(n-1) + a_{n-1} \geq A(f(n-1) + a_{n-1}) = A(f(n))$. Also $A(f(n)) = 1 + a_1 + a_2 + \ldots + a_{n-1}$ and from (1.2.3) we have $a_j \geq \alpha f(j+1) - \alpha f(j)$. Hence

$$a_{n-1} + f(n-1) \geq A(f(n)) \geq 1 + \alpha \sum_{j=1}^{n-1} f(j+1) - f(j) \geq \alpha f(n)$$

We therefore have

$$\frac{a_{n-1}}{f(n)} + \frac{f(n-1)}{f(n)} \geq \frac{A(f(n))}{f(n)} \geq \alpha$$

so that

$$\liminf_{n \to \infty} \left(\frac{a_{n-1}}{f(n)} + \frac{f(n-1)}{f(n)} \right) \geq \liminf_{n \to \infty} \frac{A(f(n))}{f(n)} \geq \alpha .$$

This, with (1.2.7), yields

$$\liminf_{n \to \infty} \frac{A(f(n))}{f(n)} = \alpha .$$

Hence

(1.2.10) $$d(A) \leq \alpha .$$

Let m be a positive integer and let $f(n-1) < m \leq f(n)$ If $m \in A$ we have $f(n-1) < m \leq f(n-1) + a_{n-1}$ so that

$$\frac{A(m)}{m} = \frac{A(f(n-1)) + m - f(n-1)}{m + f(n-1) - f(n-1)} \geq \frac{A(f(n-1))}{f(n-1)} \geq \alpha$$

If $m \notin A$, then $f(n-1) + a_{n-1} < m \leq f(n)$ so that

$$\frac{A(m)}{m} = \frac{A(f(n))}{m} \geq \frac{A(f(n))}{f(n)} \geq \alpha .$$

This implies

(1.2.11) $$d(A) \geq \alpha .$$

From (1.2.10) and (1.2.11) we get $d(A) = \alpha$. Similarly $d(B) = \beta$.

We go on to show that $d(C) = \gamma$. If $a \in A$ and $a \leq f(n)$, then $a \leq f(n-1) + a_{n-1}$. Similarly, if $b \in B$ and $b \leq f(n)$, then $b \leq f(n-1) + b_{n-1}$. Hence

$$C(f(n)) \leq 2f(n-1) + a_{n-1} + b_{n-1} .$$

Using (1.2.4) we get

$$C(f(n)) \leq 2f(n-1) + \gamma f(n) - \gamma f(n-1) + 2.$$

Hence

$$\frac{C(f(n))}{f(n)} \leq \frac{2f(n-1)}{f(n)} + \gamma - \frac{\gamma f(n-1)}{f(n)} + \frac{2}{f(n)} .$$

It follows that

$$\liminf_{n \longrightarrow \infty} \frac{C(f(n))}{f(n)} \leq \gamma$$

and hence that

$$d(C) \leq \gamma . \tag{1.2.12}$$

Let m be any positive integer. Either $C(m) = m \geq \gamma m$, in which case we have finished, or $C(m) < m$. If the latter is true, let z be the largest positive integer not exceeding m and not occurring in C. Then we have

$$\frac{C(m)}{m} = \frac{C(z) + m - z}{m} \geq \frac{C(z) + (m - z) - (m - z)}{m - (m - z)} = \frac{C(z)}{z} \tag{1.2.13}$$

Define n by $f(n-1) < z \leq f(n)$. Since $z \notin A$ and $z \notin B$ we have

$$\frac{C(z)}{z} \geq \frac{A(z) + B(z)}{z} = \frac{A(f(n)) + B(f(n))}{z} \geq \frac{A(f(n)) + B(f(n))}{f(n)} . \tag{1.2.14}$$

Now

$$(1.2.15)\quad A(f(n)) + B(f(n)) = 2 + \sum_{j=1}^{n-1} a_i + b_j \geq 2 + \gamma \sum_{j=1}^{n-1} f(j+1) - f(j)$$

$$= 2 + \gamma f(n) - \gamma f(1) \geq \gamma f(n),$$

where we have used (1.2.8), (1.2.9), (1.2.4) and the definition of f.

Using (1.2.13), (1.2.14) and (1.2.15) we get

$$\frac{C(m)}{m} \geq \gamma .$$

This together with (1.2.13) implies that $d(C) = \gamma$. The proof of the theorem is complete.

Cheo, in proving the above theorem, takes $f(n) = n!$ and this function obviously satisfies properties (i) to (iv). Our approach has the advantage that it enables us to construct more than one example of sets A and B which satisfy the given conditions (in fact, we may construct infinitely many) whereas Cheo's construction affords only one example.

3. <u>Generalizations of the $\alpha + \beta$ Theorem</u>

Consider n sets $A_1, A_2, \ldots, A_n$, not necessarily distinct. Let r be a positive integer. If $r \leq n$, by a sum of rank r of the sets $A_1, A_2, \ldots, A_n$ is meant a set $A_{i_1} + A_{i_2} + \ldots + A_{i_r}$, where $i_1, i_2, \ldots, i_r$ are r different integers not exceeding n. For $r \leq n$, the number of sums of rank r of n sets is clearly $\binom{n}{r}$. If $r > n$, by a sum of rank r of the sets $A_1, A_2, \ldots, A_n$ is meant the empty set V. Let m be an integer. Let, for $r \leq n$,

$$\varphi_r(m) = \sum_S S(m) \tag{1.3.1}$$

where the summation is over the $\binom{n}{r}$ sums of rank r of the sets $A_1, A_2, \ldots, A_n$. For example, if $n = 4$, then

$$\varphi_2(m) = \sum_{1 \le i < j \le 4} [A_i + A_j](m)\ , \quad \varphi_4(m) = [A_1 + A_2 + A_3 + A_4](m).$$

For $r > n$, define $\varphi_r(m) = 0$. We discuss the following theorem due to F. J. Dyson [10].

<u>Theorem 1.3.1</u> Let g be a positive integer. Let $\alpha \geq 0$ be such that

$$\varphi_1(m) = A_1(m) + A_2(m) + \ldots + A_n(m) \geq \alpha m, \quad m = 1, 2, \ldots, g. \tag{1.3.2}$$

Then

$$\varphi_r(m) = \binom{n-1}{r-1} \gamma m\ , \quad m = 1, 2, \ldots, g \quad r = 1, 2, \ldots, n \tag{1.3.3}$$

and where $\gamma = \mathrm{MIN}(1, \alpha)$.

<u>Remark</u>. Let $d(A_i) = \alpha_i$ for $i = 1, 2, \ldots, n$ and let $\alpha = \sum_{i=1}^{n} \alpha_i$

Then $\varphi_1(m) \geq \alpha m$ for all m. By Theorem 1.3.1, $\varphi_r(m) \geq \binom{n-1}{r-1} \gamma m$ for all m and $r = 1, 2, \ldots, n$. If we choose $r = n$, then $[A_1 + A_2 + \ldots + A_n](m) \geq \gamma m$ for all m. This implies $d(A_1 + A_2 + \ldots + A_n) \geq \gamma$, i.e. $d(A_1 + A_2 + \ldots + A_n) \geq \alpha$ if $\alpha \leq 1$ or $d(A_1 + A_2 + \ldots + A_n) = 1$ if $\alpha > 1$. This is Theorem 1.1.3. The $\alpha + \beta$ theorem is included as the special case where $n = 2$.

Proof of Theorem 1.3.1: The proof is by induction. The Theorem is clearly true for $n = 1$. Henceforth we assume that the Theorem is true for all values of n less than the actual value and that $n \geq 2$. There are two cases to be considered.

Case 1. $A_n(g) = 0$.

Let $\varphi_r'(m)$ be defined with respect to the sets $A_1, A_2, \ldots,$ A_{n-1} just as $\varphi_r(m)$ was defined with respect to $A_1, A_2, \ldots, A_n$. Since $A_n(g) = 0$, $\varphi_1'(m) = \varphi_1(m) \geq \alpha m$, $m = 1, 2, \ldots, g$. By the induction hypothesis applied to $A_1, \ldots, A_{n-1}$ it follows that

$$(1.3.4) \qquad \varphi_r'(m) \geq \binom{(n-1)-1}{r-1}\gamma m, \quad m = 1, 2, \ldots, g; \quad r = 1, 2, \ldots, n-1$$

Let S be any sum of rank r of the sets $A_1, A_2, \ldots, A_n$. S may be one of two types, namely: S can be a sum of rank r of the sets $A_1, A_2,$ $\ldots, A_{n-1}$, or S can be a sum of the form $S' + A_n$ where S' is a sum of rank $r - 1$ of the sets $A_1, A_2, \ldots, A_{n-1}$. If S is of the second type, then since $A_n(g) = 0$, we have $S(m) = S'(m)$ for $m = 1, 2, \ldots, g$. Since the above classification of sums of rank r is mutually exclusive and exhaustive we have

$$(1.3.5) \qquad \varphi_r(m) = \sum_S S(m) + \sum_{S'} S'(m), \quad m = 1, 2, \ldots, g$$

where the sums extend over the sums of $A_1, A_2, \ldots, A_{n-1}$ of ranks r and $r - 1$ respectively. From (1.3.5) and the definition of $\varphi_r'(m)$ we have

$$(1.3.6) \qquad \varphi_r(m) = \varphi_r'(m) + \varphi_{r-1}'(m), \quad m = 1, 2, \ldots, g.$$

(1.3.6) and (1.3.4) yield

$$\varphi_r(m) \geq \binom{n-2}{r-1} \gamma m + \binom{n-2}{r-2}\gamma m = \binom{n-1}{r-1} \gamma m \text{ for}$$

$m = 1, 2, \ldots, g$ which is (1.3.3). The theorem is therefore true for the actual value of n when $A_n(g) = 0$.

<u>Case 2</u>. $A_n(g) > 0$.

We assume that the theorem is true for all values of $A_n(g)$ less than the actual value. Let a, ℓ, and c be integers satisfying the following conditions:

(i) $c \in A_n$ and $c \leq g$

(ii) $1 \leq \ell < n$

(iii) either $a = 0$ or $a \in A_\ell$ or $a > g$

(iv) either $a + c \notin A_\ell$ or $a + c > g$.

That such integers a, ℓ and c exist follows from the fact that $A_n(g) > 0$, $n \geq 2$ and we may choose $a = g + 1$, say. Let a_o be the smallest a for which integers ℓ and c can be found satisfying conditions (i) to (iv). Let ℓ_o be fixed as one of the values of ℓ for which integers c exist satisfying (i) to (iv) with $a = a_o$. Let T be the set of all such integers c. We may assume that $\ell_o = 1$ since we may permute the sets $A_1, \ldots, A_{n-1}$ in any way that we please. Since $c \in A_n$, we have $T \subset A_n$. Let $A_n{*} = A_n \cap \overline{T}$, where by $\overline{T}$ we mean the set of all positive integers which do not belong to T. Let $A_1{*} = A_1 \cup \{a_o + c;\ c \in T\}$. For values of i such that $2 \leq i \leq n - 1$, let $A_i{*} = A_i$. Define $\varphi_r{*}(m)$ in terms of the sets $A_1{*}, A_2{*}, \ldots, A_n{*}$ just as $\varphi_r(m)$ was defined in terms of $A_1, A_2, \ldots, A_n$. Since $T(g) > 0$ and $T \subset A_n$, we have $A_n{*}(g) < A_n(g)$. Hence, by the induction hypothesis, the theorem is true when the sets $A_1, A_2, \ldots, A_n$ are replaced by

$A_1^*, A_2^*, \ldots, A_n^*$. Our main goals are therefore as follows. Firstly, we want to show that $\varphi_1^*(m) \geq \gamma m$ for $m = 1, 2, \ldots, g$. It will then follow by induction that $\varphi_r^*(m) \geq \binom{n-1}{r-1} \gamma m$ for $m = 1, 2, \ldots, g$. Secondly, we must show that $\varphi_r(m) \geq \varphi_r^*(m)$ for $m = 1, 2, \ldots, g$. We set out to achieve our second goal first.

<u>Lemma 1.3.1</u> $\varphi_r(m) \geq \varphi_r^*(m)$, for $m = 1, 2, \ldots, g$.

<u>Proof</u>: We may separate the sums S of rank r of the sets $A_1, A_2, \ldots, A_n$ into four mutually exclusive classes as follows:

(I) sums S of rank r of the sets $A_2, \ldots, A_{n-1}$

(II) sums of the form $S' + A_n$ where S' is a sum of rank $r - 1$ of the sets $A_2, \ldots, A_{n-1}$

(III) sums of the form $S' + A_1$ where S' is defined as in (II)

(IV) sums of the form $S'' + A_1 + A_n$ where S'' is a sum of rank $r - 2$ of the sets $A_2, \ldots, A_{n-1}$.

We therefore have

$$(1.3.7) \quad \varphi_r(m) = \sum_S S(m) + \sum_{S'} \Big\{[S' + A_1](m) + [S' + A_n](m)\Big\} + \sum_{S''} [S'' + A_1 + A_n](m)$$

for $m = 1, 2, \ldots, g$, and since $A_i^* = A_i$ for $i \neq 1$ and $i \neq n$, we have

$$(1.3.8) \quad \varphi_r^*(m) = \sum_S S(m) + \sum_{S'} \Big\{[S' + A_1^*](m) + [S' + A_n^*](m)\Big\} + \sum_{S''} [S'' + A_1^* + A_n^*](m)$$

for $m = 1, 2, \ldots, g$. Since our object is to show that $\varphi_r(m) \geq \varphi_r^*(m)$, it is clear from equations (1.3.7) and (1.3.8) that it is sufficient to show

$$(1.3.9)\quad [S' + A_1*](m) - [S' + A_1](m) \leq [S' + A_n](m) - [S' + A_n*](m)$$

for $m = 1, 2, \dots, g$, and

$$(1.3.10)\quad [S'' + A_1* + A_n*](m) \leq [S'' + A_1 + A_n](m) .$$

Let U and W be sets satisfying the following conditions:

(1) $U \subset W$

(2) if $h \leq g$ and $h \in U + A_1*$, then $h \notin W + A_1$.

We shall prove that $h - a_o \in U + A_n$ and $h - a_o \notin W + A_n*$. Now $h \in U + A_1*$ implies that $h = u + a_1*$, where $u \in U$ or $u = 0$, $a_1* \in A*$ or $a_1* = 0$ and not both u and a_1* zero. Suppose $a_1* = 0$. Then $h \in U \subset W \subset W + A_1$, which is false. It follows that $a_1* \in A_1*$. By the definition of A_1*, we must have either $a_1* \in A_1$ or $a_1* = a_o + c$, where $c \in T$. The first possibility implies that $h = u + a_1* \in U + A_1 \subset W + A_1$. Since this contradicts (2) we must have $a_1* = a_o + c$. Therefore $h - a_o = u + c \in U + T \subset U + A_n$. We go on to prove the second half of our assertion, namely that $h - a_o \notin W + A_n*$. Assume that $h - a_o \in W + A_n*$. Then $h - a_o = w + a_n*$ where $w \in W$ or $w = 0$, $a_n* \in A_n*$ or $a_n* = 0$ and not both w and a_n* are zero. Since $w \geq 0$, we have $a_o + a_n* \leq h \leq g$. It is clear from (ii) that $a_n* = 0$ implies that $h = w + a_o \in W + A_1$, which is false. We must therefore have $a_n* \in A_n*$ or equivalently, $a_n* \in A_n$ and $a_n* \notin T$. Now $a_o + a_n* \notin A_1$ implies, by (iii) that $a_n* \in T$. Since this is not the case we must have $a_o + a_n* \in A_1$. Hence $h = w + (a_o + a_n*) \in W + A_1$. This clearly contradicts (2). Our assumption that $h - a_o \in W + A_n*$ is false. Hence $h - a_o \notin W + A_n*$. We have shown that for every element h not exceeding g in $U + A_1*$ but not in $W + A_1$, there is an element

$h - a_o$ in $U + A_n$ and not in $W + A_n^*$. Hence we may assert

$$(1.3.11)\quad [U + A_1^*](m) - [W + A_1](m) \leq [U + A_n](m) - [W + A_n^*](m)$$

for $m = 1, 2, \dots , g$. Setting $U = W = S'$ in (1.3.11) yields (1.3.9). Let $h \leq g$, $h \in A_1^* + A_n^*$ and $h \notin A_1 + A_n$. Choose $U = A_n^*$ and $W = A_n$. This is allowable since $A_n^* \subset A_n$. Then we have $h - a_o \in A_n^* + A_n$ and $h - a_o \notin A_n + A_n^*$, which is absurd. It follows that if $h \in A_1^* + A_n^*$ then $h \in A_1 + A_n$ and hence that equation (1.3.10) holds. From (1.3.7), (1.3.8), (1.3.9) and (1.3.10) we get $\varphi_r(m) \geq \varphi^*(m)$ for $m = 1, 2, \dots , g$. The lemma is established.

<u>Lemma 1.3.2</u> Let $m \leq g$. Then $\varphi_1^*(m) \geq \gamma m$.

<u>Proof</u>: By definition of the A_i^* we have

$$A_i^*(m) = A_i(m) \quad \text{for } i = 2, 3, \dots , n - 1$$
$$A_1^*(m) = A_1(m) + T(m - a_o)$$
$$A_n^*(m) = A_n(m) - T(m) .$$

Hence

$$(1.3.12)\qquad \varphi_1^*(m) = \varphi_1(m) - T(m) + T(m - a_o).$$

If $T(m) = T(m - a_o)$, then $\varphi_1^*(m) = \varphi_1(m) \geq \alpha m \geq \gamma m$ and we have finished. Henceforth we assume $T(m) > T(m - a_o)$. Then there exists a least integer $t_o \in T \subset A_n$ such that $m - a_o < t_o \leq m \leq g$. By the minimal property of t_o, $A_n(t_o - 1) = A_n(m - a_o)$. Since $T \subset A_n$, we have $T(m) - T(m - a_o) \leq A_n(m) - A_n(m - a_o) = A_n(m) - A_n(t_o - 1)$. This together with (1.3.12) yields

$$(1.3.13)\qquad \varphi_1^*(m) \geq \varphi_1(m) - A_n(m) + A_n(t_o - 1).$$

Let z and c be any two integers such that $c \in A_n$ and

$$(1.3.14) \qquad z - a_o < c \leq z \leq g.$$

Such integers c and z exist since $A_n(g) > 0$ and we can choose $z = c$. Let j be a positive integer such that $1 \leq j < n$. Let $a \leq z - c$ be an integer such that either $a = 0$ or $a \in A_j$. From (1.3.14) it follows that $a \leq z - c < a_o$. Suppose $a + c \notin A_j$. Then the integers a, j, c satisfy conditions (i) to (iv), but $a < a_o$ contradicts the minimal property of a_o. Hence $a + c \in A_j$ whenever $a = 0$ or $a \in A_j$ and $a \leq z - c$. There are $A_j(z - c) + 1$ such a's. We have therefore

$$(1.3.15) \quad A_j(z) \geq A_j(c - 1) + 1 + A_j(z - c) \qquad j = 1, 2, \ldots, n - 1$$

Choose $z = m$. $c = t_o$ in (1.3.15). Then

$$A_j(m) \geq A_j(t_o - 1) + 1 + A_j(m - t_o) \quad j = 1, 2, \ldots, n - 1.$$

Summing, we get

$$\sum_{j=1}^{n-1} A_j(m) \geq \sum_{j=1}^{n-1} A_j(t_o - 1) + n - 1 + \sum_{j=1}^{n-1} A_j(m - t_o).$$

Hence

$$\varphi_1(m) - A_n(m) \geq \varphi_1(t_{o - 1}) - A_n(t_o - 1) + n - 1 + \varphi_1(m - t_o) - A_n(m - t_o).$$

Using this and the fact that $\varphi_1(t_o - 1) \geq \alpha(t_o - 1)$ in (1.3.13) we get

$$(1.3.16) \quad \varphi_1{*}(m) \geq \alpha(t_o - 1) + \varphi_1(m - t_o) - A_n(m - t_o) + n - 1.$$

Assume that there exist positive integers x such that

$$(1.3.17) \qquad x < a_o; \quad \varphi_1(x) - A_n(x) < \gamma x; \quad x \leq g .$$

Let z be the smallest such x. If $A_n(z) = 0$ then (1.3.17) implies $\varphi_1(z) < \gamma z$. But $\varphi_1(z) \geq \alpha z$, by the hypothesis of the theorem. Hence $(\gamma - \alpha)z > 0$ which is false since $\gamma \leq \alpha$. Thus $A_n(z) > 0$ and there exists an integer $c \in A_n$ not exceeding z. Since $z < a_o$, we have $z - a_o < 0 < c \leq z \leq g$, so that (1.3.14) holds. Hence (1.3.15) holds. Summing as before we get

$$(1.3.18) \quad \varphi_1(z) - A_n(z) \geq \varphi_1(z - c) - A_n(z - c) + \varphi_1(c - 1) - A_n(c - 1) + n - 1.$$

Now $z - c < z$ and $c - 1 < z$ and since z is the smallest integer satisfying $\varphi_1(z) - A_n(z) < \gamma z$, we have $\varphi_1(z - c) - A_n(z - c) \geq \gamma(z - c)$ and $\varphi_1(c - 1) - A_n(c - 1) \geq \gamma(c - 1)$. This, together with (1.3.18), implies

$$(1.3.19) \quad \varphi_1(z) - A_n(z) \geq \gamma z - \gamma + n - 1 \geq \gamma z - \gamma + 1.$$

Then (1.3.17) and (1.3.19) yield $0 > -\gamma + 1$, which is false since $\gamma \leq 1$. The assumption that (1.3.17) is satisfied by positive integers x is therefore incorrect.

Recall that $m - a_o < t_o \leq m \leq g$, so that $m - t_o < a_o$ and $m - t_o \leq g$. Hence $m - t_o$ satisfies the first and third parts of (1.3.17). It cannot satisfy the second part. We therefore have

$$(1.3.20) \qquad \varphi_1(m - t_o) - A_n(m - t_o) \geq \gamma(m - t_o).$$

(1.3.16) and (1.3.20) yield

$$\varphi_1^*(m) \geq \gamma(m - t_o) + \alpha(t_o - 1) + n - 1.$$

This may be written as

$$\varphi_1^*(m) \geq \gamma m + (\alpha - \gamma)(t_o - 1) + n - 1 + \gamma.$$

Since $n \geq 2$ and $\gamma \leq 1$, then $n - 1 - \gamma \geq 0$. Also since $t_o \in A_n$, and $\alpha - \gamma \geq 0$, we have $(\alpha - \gamma)(t_o - 1) \geq 0$. Hence $\varphi_1^*(m) \geq \gamma m$ and the lemma is established.

We proceed to the proof of the theorem. If $\alpha \leq 1$, then $\gamma = \alpha = \text{MIN}(1, \alpha) = \text{MIN}(1, \gamma)$ and if $\alpha > 1$, then $\gamma = 1 = \text{MIN}\ (1, \gamma)$. Hence, by the induction hypothesis applied to the sets $A_1^*, A_2^*, \ldots,$ A_n^*, we have

$$\varphi_r^*(m) \geq \binom{n-1}{r-1} \gamma m \quad \text{for} \quad m = 1, 2, \ldots, g; \quad r = 1, 2, \ldots, n.$$

By Lemma 1.3.1

$$\varphi_r(m) \geq \binom{n-1}{r-1} \gamma m \quad \text{for} \quad m = 1, 2, \ldots, g; \quad r = 1, 2, \ldots, n$$

which is (1.3.3)

<u>Corollary</u>: For each pair of integers r and m such that $r \leq n$, $m \leq g$, there exists a set of r different integers $i_1, i_2, \ldots, i_r$ not exceeding n and a sum $S = A_{i_1} + A_{i_2} + \ldots + A_{i_r}$ such that

(1.3.22) $$S(m) \geq \frac{r}{n} \gamma m$$

Proof: We have $\varphi_r(m) \geq \binom{n-1}{r-1} \gamma m$, where $\varphi_r(m)$ contains $\binom{n}{r}$ terms. Let $S(m) = (A_{i_1} + A_{i_2} + \ldots + A_{i_r})(m)$ be the largest of these. Then

$$\binom{n}{r} S(m) \geq \binom{n-1}{r-1} \gamma m$$

which implies (1.3.22).

Note that in particular when $r = n$, $S(m) \geq \gamma m$ for $m = 1, 2, \ldots, g$, which again implies Theorem 1.1.3 and the $\alpha + \beta$ theorem.

4. Essential Components

A set A is said to be an essential component if for every set B with $0 < d(B) < 1$, $d(A + B) > d(B)$. It is obvious from the $\alpha + \beta$ theorem that if A has positive density then A is an essential component. Khinchin [20] proved that the squares are an essential component thus giving an example of a set of density zero which is an essential component. We prove this fact here. In fact, we prove considerably more. Recall that a set A is said to be a basis of order k if every positive integer can be expressed as a sum of at most k elements of A. The set of squares is a basis of order 4. The following theorem is due to Erdös [11].

Theorem 1.4.1 Every basis is an essential component.

Proof: Let A be a basis of order k and let $d(B) = \beta > 0$. We shall prove that

$$d(A + B) \geq \beta + \frac{\beta(1 - \beta)}{2k} . \qquad (1.4.1)$$

Let n be a positive integer. Let $n_1 < n_2 < \ldots < n_t \leq n$ be the positive integers not exceeding n and which do not occur in B. Put

$$e = n_1 + n_2 + \ldots + n_t - \frac{t(t+1)}{2}. \tag{1.4.2}$$

Since $n_1 \geq 1$, $n_2 \geq 2$, $\ldots$, $n_t \geq t$, we have $e \geq 0$. The idea of the proof is as follows. We shall show that $A + B$ contains at least $B(n) + \frac{e}{kn}$ integers not exceeding n. We shall then show that the lower bound 0 on e can be substantially improved.

Consider the equation $b + c = n_j$, where $b \in B$, $b \leq n$ and where c is a positive integer. (Throughout the remainder of the proof the symbol b will have this meaning, i.e. $b \in B$, $b \leq n$.) For each value of j, $1 \leq j \leq t$, there are $n_j - j$ solutions in b and c. This follows from the fact that the number of b's less than n_j is $n_j - j$ and every b gives one solution. The total number of solutions is therefore

$$\sum_{j=1}^{t} (n_j - j) = e.$$

Now there are at most n possible values for c, namely $1, 2, \ldots , n$. Hence, for at least one value of c, say $c = r$, there are not less than e/n solutions of $b + r = n_j$, i.e. there are at least e/n of the numbers $n_1, n_2, \ldots , n_t$ in the set $\{b + r\}$.

Since A is a basis of order k we may write $r = a_1 + a_2 + \ldots + a_k$ where the a's are either zero or in A and not all of the a's are zero. Let μ_s be the number of the n_j in the set $\{b + a_s\}$. In the set $\{b + a_1\}$ there are μ_1 of the n_j together with some b's.

(Any element of $\{b + a_1\}$ which is not an n_j is a b.) If we add a_2 to the numbers in $\{b + a_1\}$, the μ_1 of the n_j give at most μ_1 of the n_j and the b's give at most μ_2 of the n_j. Hence $\{b + a_1 + a_2\}$ contains at most $\mu_1 + \mu_2$ of the n_j. This argument can be applied repeatedly and we see that $\{ b + a_1 + a_2 + \dots + a_k\} = \{b + r\}$ contains at most $\mu_1 + \mu_2 + \dots + \mu_k$ of the n_j. But $\{b + r\}$ contains at least e/n of the n_j. Hence for one of the μ's, say μ_ℓ, we have $\mu_\ell \geq e/kn$. Hence the set $\{b + a_\ell\}$ contains at least e/kn of the n_j. The set $\{b\}$ contains $B(n)$ b's. Since b's and the n_j are all different, $A + B$ contains at least $B(n) + e/kn$ integers not exceeding n. Now

$$n_j - j = B(n_j) \geq \beta n_j$$

so that

$$n_j \geq \frac{j}{1 - \beta} . \tag{1.4.3}$$

Using (1.4.2) and (1.4.3) we have

$$e \geq \frac{1 + 2 + \dots + t}{1 - \beta} - \frac{t(t + 1)}{2} = \frac{t(t + 1)}{2} \left\{\frac{\beta}{1 - \beta}\right\} . \tag{1.4.4}$$

Let $C = A + B$. Then

$$C(n) \geq B(n) + \frac{e}{kn} \geq B(n) + \frac{t(t + 1)}{2kn} \left\{\frac{\beta}{1 - \beta}\right\} .$$

Replacing $t(t + 1)$ by t^2 and noting that $t = n - B(n)$, we have

$$\frac{C(n)}{n} \geq \frac{B(n)}{n} + \frac{\beta(n - B(n))^2}{2kn^2 (1 - \beta)} . \tag{1.4.5}$$

It is easy to check that for $x \geq \beta n$ the function

$$f(x) = \frac{x}{n} + \frac{\beta(n - x)^2}{2kn^2(1 - \beta)}$$

is increasing. This, with (1.4.5) and the fact that $B(n) \geq \beta n$, implies that

$$\frac{C(n)}{n} \geq \beta + \frac{\beta(1 - \beta)}{2k} .$$

The theorem follows.

Erdös [15] conjectured that (1.4.1) can be improved to

$$d(A + B) \geq \beta + \frac{\beta(1 - \beta)}{k}$$

but later showed by a probabilistic argument that this is not the case. However, some improvements over (1.4.1) have been made. One line of approach is to take into consideration the fact that for a given basis A of order k, many integers can be expressed as the sum of fewer than k elements of A. Let $m = a_1 + a_2 + \ldots + a_h$ be a representation of m as the sum of integers in A and let $h = h(m)$ be the smallest number for which such a representation is possible. Let

$$\lambda = \operatorname*{l.u.b}_{n \geq 1} \frac{1}{n} \sum_{m=1}^{n} h(m).$$

Landau [24] showed that

$$d(A + B) \geq \alpha + \frac{\alpha(1 - \alpha)}{2\lambda}$$

and Brauer [3] proved

$$d(A + B) \geq \alpha + \frac{\alpha(1 - \sqrt{\alpha})}{\lambda} .$$

Further results and references to the literature on the subject can be found in a paper by Kasch [19].

Linnik [26] found an example of an essential component which is not a basis, thus disproving the converse of Theorem 1.4.1. Erdös [16] conjectured that any set which is lacunary, i.e. $a_{k+1} > ca_k$ where $c > 1$, cannot be an essential component. If $a_k = o(a_{k+1})$ it follows from Theorem 1.3.1 that the set consisting of the a_k is not an essential component. However, the conjecture of Erdös has not been settled and there does not seem to be any conjecture giving necessary and sufficient conditions for a set to be an essential component.

5. Modified Schnirelmann Density and Besicovitch Density

The definition of Schnirelmann density has the disadvantage that if $1 \notin A$, then $d(A) = 0$. We remedy this situation to some extent by defining two new densities of A as follows.

$$\alpha^* = d^*(A) = \underset{n \in A}{\text{g.l.b.}} \frac{A(n)}{n} \tag{1.5.1}$$

if A is an infinite set. We agree that if A is finite then $\alpha^* = 0$. If $A \neq J$, let s be the smallest positive integer missing from A. Let

$$\alpha_1 = d_1(A) = \underset{n \geq s}{\text{g.l.b.}} \frac{A(n)}{n+1} . \tag{1.5.2}$$

We agree that if $A = J$, then $\alpha_1 = 1$. α_1 is called the Besicovitch density of A and α^* is called the modified Schnirelmann density. We prove the following result due to H. B. Mann [29] which, in addition to being of interest in itself, will enable us to prove the analogue of the $\alpha + \beta$ theorem for Besicovitch density. Let $C = A + B$ and let β_1 and γ_1 be defined for B and C just as α_1 was defined for A.

<u>Theorem 1.5.1</u> Let $n \notin C$ and let $n_1 < n_2 < \ldots < n_r = n$ be the integers not exceeding n and which are not in C. Then

$$(1.5.3) \quad C(n) \geq \mathrm{MAX} \left\{ \alpha_1 n + B(n) + \min_{n_i \leq n} [A(n_i) - \alpha_1 n_i], \right.$$

$$\left. A(n) + \beta_1 n + \min_{n_i \leq n} [B(n_i) - \beta_1 n_i] \right\} .$$

<u>Proof</u>: Let $n - n_i = d_i$ for $i < r$. Suppose there is at least one $b \in B$, or $b = 0$, such that $a + b + d_i = n_j$ for some $a \in A$, or $a = 0$, $i < r$ and $j < r$. Let b_o be the smallest $b \in B$, or $b_o = 0$, for which this is so. Form all numbers $b_o + d_t$ for which $a + b_o + d_t = n_s$ has solutions $a \in A$ or $a = 0$, $t < r$, $s < r$. Put $B^* = \{b_o + d_t\}$. Then

$$(1.5.4) \qquad B \cap B^* = V,$$

for if $b_o + d_j \in B^*$, then $b_o + d_j \in B$ implies $n_i = a + (b_o + d_j)$ is in C, which is not the case. Also for any $s < r$ we have

$$(1.5.5) \qquad n \neq a + b_o + d_s ,$$

for if $n = a + b_o + d_s$, then since $d_s = n - n_s$ we have $n_s = a + b_o \in A + B = C$, which is false. Let $B \cup B^* = B_1$ and let $A + B_1 = C_1$. We shall prove

$$(1.5.6) \qquad C_1(n) - C(n) = B_1(n) - B(n) = B^*(n) > 0.$$

We have $B_1 = B \cup B^*$, $B \cap B^* = V$ so that $B_1(n) = B(n) + B^*(n)$, i.e. $B_1(n) - B(n) = B^*(n)$. Let $b_o + d_t \in B^*$. Then $a + b_o + d_t = n_s$ for some $a \in A$ or $a = 0$, $s < r$. Using $d_t = n - n_t$, $d_s = n - n_s$,

this gives $a + b_o + d_s = n_t$. Hence $n_t \notin C$, $n_t \in C_1$. Conversely, let $n_t \notin C$, $n_t \in C_1$. Then $n_t = a + b_o + d_m$ for some $a \in A$ or $a = 0$ and $m < r$. Hence $n_m = a + b_o + d_t$ which implies $b_o + d_t \in B^*$. The correspondence $b_o + d_t \longleftrightarrow n_t$ where $b_o + d_t \in B^*$, $n_t \notin C$ and $n_t \in C_1$ is one to one. Hence among the positive integers not exceeding n, B^* contains as many numbers as there are integers missing from C and preceding n and which are missing from C_1. Hence $C_1(n) - C(n) = B^*(n)$ and the proposition follows.

Combining (1.5.4), (1.5.5) and (1.5.6) we get the following lemma.

<u>Lemma 1.5.1</u> If there exists at least one equation of the form $a + b + d_i = n_j$, then there exists a set $B_1 \supset B$ such that $C_1 = A + B_1$ does not contain n and $C_1(n) - C(n) = B_1(n) - B(n) > 0$.

We proceed to prove

$$(1.5.7) \qquad C(n) \geq \alpha_1 n + B(n) + \min_{n_i \leq n} \{A(n_i) - \alpha_1 n_i\}$$

Clearly $C(n_1) = n_1 - 1$ as n_1 is the smallest integer not in C. By Lemma 1.1.1 we have $A(n_1) + B(n_1) \leq n_1 - 1$. Hence $C(n_1) \geq A(n_1) + B(n_1) = \alpha_1 n_1 + B(n_1) + \{A(n_1) - \alpha_1 n_1\}$, so that (1.5.7) is true when $n = n_1$. We assume that (1.5.7) is true for the case when n is the j th missing integer in C, $j < r$, and proceed by induction on j. There are two possibilities.

<u>Case 1</u>. $d_{r-1} \leq n_1$.

Then $n_1 - d_{r-1} < n_1$ as $d_{r-1} > 0$. Hence $n_1 - d_{r-1} \in C$ or is zero. We have therefore $n_1 - d_{r-1} = a + b$, where $a \in A$ or $a = 0$

and $b \in B$ or $b = 0$. The condition of Lemma 1.5.1 is satisfied. We may therefore construct sets B_1 and $C_1 = A + B_1$ as outlined above. Let n be the j th gap in C_1. Then $j < r$ as C_1 has fewer gaps than C. By the induction hypothesis

$$(1.5.8) \qquad C_1(n) \geq \alpha_1 n + B_1(n) + \underset{n_i' \leq n}{\mathrm{MIN}} \{A(n_i) - \alpha_1 n_i'\},$$

where the n_i' are the integers missing from C_1. By the lemma,

$$(1.5.9) \qquad C(n) - C_1(n) = B(n) - B_1(n) \quad .$$

Adding (1.5.8) and (1.5.9) and noting that the n_i' are included among the n_i, we get (1.5.7).

<u>Case 2</u>. $d_{r-1} > n_1$.

Now $n - n_{r-1} - 1 = n - (n - d_{r-1}) - 1 = d_{r-1} - 1 \geq n_1 \geq s$, where s is the smallest positive integer missing from A. Hence

$$(1.5.10) \qquad A(n - n_{r-1} - 1) \geq \alpha_1(n - n_{r-1}).$$

The numbers z such that $n_{r-1} < z < n$ are in C. Suppose $z \in B$. Then z is not of the form $n - a$ where $a \in A$ and $a \leq (n - 1) - n_{r-1}$. Hence

$$(1.5.11) \qquad (n - 1) - n_{r-1} \geq A((n-1) - n_{r-1}) + B(n) - B(n_{r-1}) \ .$$

By the induction hypothesis

$$(1.5.12) \quad C(n_{r-1}) \geq \alpha_1 n_{r-1} + B(n_{r-1}) + \underset{n_i \leq n_{r-1}}{\mathrm{MIN}} [A(n_i) - \alpha_1 n_i] \ .$$

Adding (1.5.11) and (1.5.12) and using (1.5.10) we have, on noting that $C(n) = C(n_{r-1}) + (n - 1) - n_{r-1}$,

$$(1.5.13)\quad C(n) \geq \alpha_1 n + B(n) + \underset{n_i \leq n_{r-1}}{\text{MIN}} [A(n_i) - \alpha_1 n_i] .$$

We may replace the last term on the right by $\underset{n_i \leq n}{\text{MIN}} \{A(n_i) - \alpha_1 n_i\}$ which yields (1.5.7).

Similarly we may show that

$$(1.5.14)\qquad C(n) \geq A(n) + \beta_1 n + \underset{n_i \leq n}{\text{MIN}} \{B(n_i) - \beta_1 n_i\}.$$

(1.5.7) and (1.5.14) imply (1.5.3).

<u>Theorem 1.5.2</u> The analogue of the $\alpha + \beta$ theorem is true for Besicovitch density, i.e.

(i) if $\alpha_1 + \beta_1 \leq 1$, then $\gamma_1 \geq \alpha_1 + \beta_1$

(ii) if $\alpha_1 + \beta_1 > 1$, then $\gamma_1 = 1$.

<u>Proof</u>: (i) Let $\alpha_1 + \beta_1 \leq 1$. If $C = J$, then $\gamma_1 = 1 \geq \alpha_1 + \beta_1$ and we have finished. Hence we may assume that there are gaps in C. Let $n \notin C$. Let $A(n_\ell) - \alpha_1(n_\ell) = \underset{n_i \leq n}{\text{MIN}} \{A(n_i) - \alpha_1 n_i\}$, where we are using the notation of the preceding theorem. By (1.5.7)

$$\begin{aligned} C(n) &\geq \alpha_1 n + B(n) + A(n_\ell) - \alpha_1 n_\ell \\ &\geq \alpha_1 n + \beta_1(n + 1) + \alpha_1(n_\ell + 1) - \alpha_1 n_\ell \\ &= (\alpha_1 + \beta_1)(n + 1) \quad . \end{aligned}$$

If $n \in C$, let n' be the largest positive integer not in C and not exceeding n. We may, by virtue of the definition of Besicovitch density, assume that such an n' exists. Then

$$\frac{C(n)}{n+1} = \frac{C(n') + n - n'}{n+1} \geq \frac{C(n') + (n - n') - (n - n')}{(n+1) - (n - n')} = \frac{C(n')}{n' + 1} \geq \alpha_1 + \beta_1 .$$

Hence $\frac{C(n)}{n+1} \geq \alpha_1 + \beta_1$ for all $n \geq s$, where s is the smallest integer not in C. Hence $\gamma_1 \geq \alpha_1 + \beta_1$.

(ii) Let $\alpha_1 + \beta_1 > 1$. Assume $C \neq J$ and let $n \notin C$. We have, as in part (i), $C(n) \geq (\alpha_1 + \beta_1)(n+1) > n+1$ which is a contradiction. Hence $C = J$ and $\gamma_1 = 1$.

Theorem 1.5.3 The analogue of the $\alpha + \beta$ theorem does not hold for the modified Schnirelmann density.

Proof: We exhibit two counterexamples.

(a) Let $A = B = \{1, 4 + j; \ j = 0, 1, 2, \ldots\}$. Then $\alpha^* = \beta^* = 1/2$ and $\alpha^* + \beta^* = 1$. Also $C = \{1, 2, 4 + j; \ j = 0, 1, 2, \ldots\}$ so that $\gamma^* = 3/4 < 1$.

(b) Let $A = B = \{1, 5 + j; \ j = 0, 1, 2, \ldots\}$. Then $\alpha^* = \beta^* = 2/5$ and $\alpha^* + \beta^* = 4/5 < 1$. Also $C = \{1, 2, 5 + j; \ j = 0, 1, 2, \ldots\}$ so that $\gamma^* = 3/5 < 4/5$.

While the analogue of the $\alpha + \beta$ theorem does not hold for modified Schnirelmann density, it is interesting to note that given α^*, β^*, γ^* such that $\alpha^* \geq 0$, $\beta^* \geq 0$, $1 \geq \gamma^* \geq \alpha^* + \beta^*$, one can construct sets A, B, and $C = A + B$ such that $d^*(A) = \alpha^*$, $d^*(B) = \beta^*$ and $d^*(C) = \gamma^*$. The proof of this fact is almost identical to Cheo's proof of a similar theorem for Schnirelmann densities, and will be omitted here.

We conclude this section by considering briefly some results of Stalley [42] on Besicovitch and modified Schnirelmann densities. The proofs of these theorems are not difficult and only one proof shall be given here.

<u>Theorem 1.5.4</u> If $\alpha^* + \beta^* > 1$, then $\gamma^* = 1$.

<u>Proof</u>: We need to show that $C = J$. Assume that $n \notin C$. Then $n \notin A$, $n \notin B$. Let $n + x$ and $n + y$ be the smallest integers in A and B respectively, larger than n. Then

$$\begin{aligned} A(n) + B(n) &= A(n + x) + B(n + y) - 2 \\ &\geq \alpha^*(n + x) + \beta^*(n + y) - 2 \\ &\geq \alpha^*(n + 1) + \beta^*(n + 1) - 2 \\ &\geq (\alpha^* + \beta^*)(n + 1) - 2 \\ &> (n - 1). \end{aligned}$$

By Lemma 1.1.1 we must have $n \in C$, which is a contradiction. Hence $C = J$ and $\gamma^* = 1$.

While $\alpha^* + \beta^* \geq 1$ does not imply $\gamma^* = 1$, and $\alpha^* + \beta^* \leq 1$ does not imply $\gamma^* \geq \alpha^* + \beta^*$, Stalley showed that if $\alpha^* + \beta \geq 1$, then $\gamma^* = 1$ and if $\alpha^* + \beta^* \leq 1$ then $\gamma^* \geq \alpha_1 + \beta^*$. He was also able to prove that if A contains 1, 2, ... , k, then $\alpha_1 \geq \frac{k}{k+1} \alpha^*$, and using this result, he showed that if $\alpha^* + \beta^* \leq 1$ and 1, 2, ... , $k \in A$, then $\gamma^* \geq \frac{k}{k+1} \alpha^* + \beta^*$.

6. <u>Some Additional Results</u>

In this section we discuss some further results related to Schnirelmann density. Davenport [8] considered the analogue of the $\alpha + \beta$ theorem for residue classes modulo p, where p is a prime. He showed that if $a_1, a_2, \ldots, a_m$ are different residue classes modulo p and if $b_1, b_2, \ldots, b_n$ is another set of different residue classes modulo p, then if we denote by $c_1, c_2, \ldots, c_\ell$ the set of different residue classes modulo p which can be written in the

form $a_i + b_j$,

(1) $\ell \geq m + n - 1$, if $m + n - 1 \leq p$

(2) $\ell = p$, if $m + n - 1 > p$.

We prove (1) by induction on n. When $n = 1$, the assertion is obvious. We find it necessary to discuss the case $n = 2$ as well. If $n = 2$, write $b_1 - b_2 = b \neq 0$ and assume that (1) is false, i.e. that $\ell < m + 1$. Now, for every a_i it is clear that $a_i + b$ is one of the a's (mod p), since if, for some fixed i, $a_i + b \equiv a_j$ (mod p) is false for $j = 1, 2, \ldots, m$, then $a_i + b_1 \equiv a_j + b_2$ (mod p) is false for $j = 1, 2, \ldots, m$, thus yielding at least $m + 1$ distinct residues of the form $a_i + b_j$. This contradicts our assumption that $\ell < m + 1$. Now kb represents all residues modulo p as k ranges from 1 to p. (Note that if p were not a prime our argument would break down here.) Suppose that for some k and some i, $a_i + kb \equiv a_j$ (mod p) is false for all j. Then $a_j - a_i \equiv kb$ (mod p) is false for all j. This is impossible by the remark made above. Hence $a_i + kb$ is one of the a's modulo p for every k. Noting that all residue classes modulo p can be represented in the form $a_i + kb$ we must have $m = p$. This contradicts the hypothesis that $m + 1 \leq p$. The theorem is therefore true when $n = 2$.

Henceforth we assume that the theorem is true for all values of n less than the actual value and that $n > 2$. We may also assume that $\ell < p$. Consider the two sets of residue classes $\{c_1, c_2, \ldots, c_\ell\}$ and $\{b_1, b_n\}$. Since the theorem has already been established for

the case where there are two b's and since $\ell + 2 - 1 \leq p$, we may conclude that there are at least $\ell + 1$ residues which are of the form $c_i + b_1$ or $c_i + b_n$. Hence there is at least one residue class d such that $d - b_1$ is a c and $d - b_n$ is not. Since we may arrange the residues $b_2, b_3, \ldots, b_{n-1}$ and $c_1, c_2, \ldots, c_\ell$ in any order that we please, we may assert that there exists an integer r where $1 \leq r \leq n$ such that $d - b_s \equiv c_s \pmod p$ for $1 \leq s \leq r$ and $d - b_t \equiv h_t \pmod p$ for $r < t \leq n$ and where $h_t \equiv c_i \pmod p$ is false for all $i = 1, 2, \ldots, \ell$. For $r < t \leq n$ and $1 \leq s \leq r$, it is clear that $c_s - b_t$ is not an a modulo p, for assuming the contrary we get $h_t \equiv a_j + b_s \pmod p$ which is false. Hence the ℓ' residue classes representable in the form $a_i + b_t$; $1 \leq i \leq m$ and $r < t \leq m$, form a subset of the c's not containing $c_1, c_2, \ldots, c_r$. Hence $\ell' \leq \ell - r$. By the induction hypothesis with $n' = n - r$ we have $\ell' \geq m + n' - 1$. This implies $\ell \geq m + n - 1$, as required.

Part (ii) of Davenport's result is much easier to prove. Let $m + n - 1 > p$ and consider the residues $b_1, b_2, \ldots, b_n$ and $a_1, a_2, \ldots, a_{p-n+1}$. Then $(p - n + 1) + n - 1 = p \leq p$. Hence by part (i) if we let $c_1, c_2, \ldots, c_{\ell'}$ be those different residue classes which can be represented in the form $a_i + b_j$; $1 \leq i \leq p - n + 1$ and $1 \leq j \leq n$, we have $\ell' \geq (p - n + 1) + n - 1 = p$. Hence $\ell' = p$ and $\ell = p$.

Further discussion of Davenport's theorem and references to the literature can be found in a paper by Chowla, Mann and Strauss in [7]. Scherk [38] has shown that a similar theorem is true for

additive groups in general. More precisely, Scherk has shown that if (i) G is an arbitrary abelian group, (ii) A and B are finite subsets of G each containing 0. (iii) $a \in A$, $b \in B$ and $a + b = 0$ implies $a = 0$, $b = 0$, then $N(A + B) \geq N(A) + N(B) - 1$ where $N(S)$ denotes the number of elements in S. We shall not give a proof of Scherk's result here.

Cheo [5] has shown that the analogue of the $\alpha + \beta$ theorem cannot in general be extended to algebraic integers. He has proved that the $\alpha + \beta$ theorem does not hold for the Gaussian integers.

CHAPTER II

ASYMPTOTIC DENSITY AND RELATED TOPICS

1. Introduction

We define the lower asymptotic density of a set A by

(2.1.1) $$\delta_1(A) = \liminf_{n \to \infty} \frac{A(n)}{n}$$

and the upper asymptotic density by

(2.1.2) $$\delta_2(A) = \limsup_{n \to \infty} \frac{A(n)}{n} .$$

If the sequence $\{\frac{A(n)}{n}\}$ has a limit, then $\delta_1(A) = \delta_2(A)$ and the common value, $\delta(A)$, is called the asymptotic density of A. We have then

(2.1.3) $$\delta(A) = \lim_{n \to \infty} \frac{A(n)}{n} .$$

2. The Analogue of the $\alpha + \beta$ Theorem

That the analogue of the $\alpha + \beta$ theorem is in general false for asymptotic density can easily be verified by taking $A = B = \{10k, k = 1, 2, \ldots\}$. Then $\delta(A) = \delta(B) = 1/10$. Also $C = \{10k, k = 1, 2, \ldots\}$ so that $\delta(C) = 1/10 < \delta(A) + \delta(B)$. Erdös [13] proved that if $1 \in B$, $\delta_1(A) + \delta_1(B) \leq 1$ and $\delta_1(B) \leq \delta_1(A)$, then $\delta_1(C) \geq \delta_1(A) + \delta_1(B)/2$. Shapiro [41] improved Erdös' result by removing the hypothesis $\delta_1(B) \leq \delta_1(A)$. Ostmann [35] proved that if B contains k consecutive integers then $\delta_1(C) \geq \delta_1(A)A + \delta_1(B)\{1 - k^{-1}\}$. We present a proof of Shapiro's result.

<u>Theorem 2.2.1</u> Let $\delta_1(A) = \alpha$, $\delta_1(B) = \beta$, $\delta_1(C) = \gamma$, $\alpha + \beta \leq 1$ and $1 \in B$. Then $\gamma \geq \alpha + \frac{\beta}{2}$.

<u>Proof</u>: If $\alpha = 0$ or $\beta = 0$, the theorem is obviously true. Henceforth we assume that α and β are both not zero. Let ϵ be a positive number such that $\alpha > \epsilon > 0$ and $\beta > \epsilon > 0$. One can then find a largest integer m such that $A(m) \leq (\alpha - \epsilon)m$. (It can occur that $m = 0$.) Let $A_\epsilon = \{a - m; \ a \in A, \ a - m > 0\}$. Let x be a positive integer. Then

$$A_\epsilon(x) = A(x + m) - A(m) \quad . \tag{2.2.1}$$

By the minimal property of m, $A(x + m) > (\alpha - \epsilon)(x + m)$. Also $-A(m) \geq -(\alpha - \epsilon)m$. Using this and (2.2.1) we get

$$A_\epsilon(x) > (\alpha - \epsilon)x. \tag{2.2.2}$$

This is true for all positive integers x. Hence the Schnirelmann density of A_ϵ is greater than $\alpha - \epsilon$. Since $\alpha - \epsilon > 0$, we have $1 \in A_\epsilon$, and by the definition of A_ϵ it follows that $m + 1 \in A$. In exactly the same way we can construct a set $B_\epsilon = \{b - \ell; \ b \in B, \ b - \ell > 0\}$ such that the Schnirelmann density is greater than $\beta - \epsilon$ and such that $\ell + 1 \in B$. Let $C_\epsilon = A_\epsilon + B_\epsilon = \{a - m, \ b - \ell, \ a + b - m - \ell\}$. The Schnirelmann density of C_ϵ is greater than $\alpha + \beta - 2\epsilon$. Hence for any positive integer x we have

$$C_\epsilon(x) \geq (\alpha + \beta - 2\epsilon)x. \tag{2.2.3}$$

Let C_ϵ' be the set obtained from C_ϵ by adding $m + \ell + 1$ to each member. Then $C_\epsilon' = \{a + \ell + 1, \ b + m + 1, \ a + b + 1\}$. It must be

remembered that the a's and b's are members of A and B respectively and are restricted so that $a - m > 0$ and $b - \ell > 0$. We have

$$(2.2.4) \quad C_\epsilon'(x) \geq C_\epsilon(x) - (m + \ell + 1) > (\alpha + \beta - 2\epsilon)x - (m + \ell + 1).$$

Since $\ell + 1 \in B$ and $m + 1 \in A$, it follows that $C_\epsilon' \subset \{a + b, a + b + 1;\ a \in A,\ b \in B\} = C'$, say, where the other restrictions on a and b are now dropped. We have therefore

$$C'(x) > (\alpha + \beta - 2\epsilon)x - (m + \ell + 1).$$

Let t be the number of the $a + b \leq x$ such that $a + b + 1 \notin \{a + b\}$. We consider two cases.

<u>Case 1</u>. $t \leq \beta x/2$.

Then there are at least $\beta x/2$ of the $a + b + 1 \in \{a + b\}$. Because of this "overlap" the number of the $a + b \leq x$ must be greater than $(\alpha + \frac{\beta}{2} - 2\epsilon)x - (m + \ell + 1)$.

<u>Case 2</u>. $t > \beta x/2$.

If $a + b + 1 \notin \{a + b\}$ then $a + b \notin A$, as $1 \in B$. Hence the set $\{a, a + b\}$ contains, for $x > m$, more than $(\alpha - \epsilon + \frac{\beta}{2})x$ different integers not exceeding x.

In Case 1 we note that $\{a + b\} \subset C$ and in Case 2 that $\{a, a + b\} \subset C$. Hence, in both cases, for sufficiently large x, C contains at least $(\alpha + \frac{\beta}{2} - 2\epsilon)x - (m + \ell + 1)$ different integers not exceeding x. Hence

$$\frac{C(x)}{x} \geq \alpha + \frac{\beta}{2} - 2\epsilon - \frac{(m + \ell + 1)}{x}.$$

and

$$\gamma = \delta_1(C) = \liminf_{x \to \infty} \frac{C(x)}{x} \geq \alpha + \frac{\beta}{2} - 2\epsilon.$$

Since ϵ is arbitrary, the theorem follows.

It is interesting to note in passing that given $\alpha \geq 0$, $\beta \geq 0$ and $1 \geq \gamma \geq \alpha + \beta$ one can construct sets A, B, $C = A + B$ such that $\delta(A) = \alpha$, $\delta(B) = \beta$ and $\delta(C) = \gamma$. The proof of this is identical with the proof of Theorem 1.2.1 for the corresponding statement about Schnirelmann densities. Indeed, the sets constructed in Theorem 1.2.1 have the same Schnirelmann and asymptotic densities.

From (1.5.4) we get $C(n) \geq \alpha_1 n + B(n)$ provided that $n \notin C$. Hence if C has infinitely many gaps, we have

$$\delta_1(C) = \liminf_{n \to \infty} \frac{C(n)}{n} = \alpha_1 + \liminf_{n \to \infty} \frac{B(n)}{n} = \alpha_1 + \delta_1(B) .$$

We therefore have the following relation between lower asymptotic densities and the Besicovitch density:

(2.2.5) $$\delta_1(C) \geq \alpha_1 + \delta_1(B) .$$

This relation was first observed by H. B. Mann [29].

3. Complementary Sets of Positive Integers

Two sets A and B are said to be complementary if every sufficiently large integer can be written in the form $a + b$, $a \in A$, $b \in B$. It was conjectured by Erdös that each infinite set A has a complementary set B of asymptotic density zero. The truth of the conjecture follows from the following much stronger theorem of Lorentz [27].

Theorem 2.3.1 Let A be an infinite set of positive integers. Then there exists a complementary set B satisfying

$$(2.3.1) \qquad B(n) \leq c\sum_{k=1}^{n} \frac{\log A(k)}{A(k)}$$

where the terms in the sum with $A(k) = 0$ or 1 are to be replaced by one and where c is an absolute constant, i.e. c does not depend on n but may depend on the set A.

To prove the theorem we need the following lemma.

Lemma 2.3.1 Let $i < j$ be positive integers such that $A(j - i + 1) \geq 2$. Then we can choose integers b in the interval $[i, 2j[$ in such a way that the sums $a + b$ where $a \in A$ completely fill the interval $]j, 2j]$. The number ℓ of these b's satisfies

$$\ell < C\,\frac{j \log A(j - i + 1)}{A(j - i + 1)}.$$

Proof: For our first b we choose an integer b_1 in $[i, 2j[$ in such a way that the subset of $A + b_1$ which is contained in $]j, 2j]$ has the greatest possible number t $(t \leq j)$ of elements. For our second b we choose an integer b_2 in $[i, 2j[$ in such a way that the subset of $A + b_2$ which is contained in $]j, 2j]$ contains the greatest possible number of elements not belonging to $A + b_1$. It can occur that b_2 yields just as many elements as b_1, but not more. This procedure is repeated. To each non-negative integer $s \leq t$ there corresponds a certain number ℓ_s (possibly zero) of b's such that $A + [b]$ contains exactly s new points in $]j, 2j]$. We shall say that these b's correspond to s. After all of the b's corresponding to $t, t - 1, \ldots, s + 1$ are chosen there will remain a set R of integers

in $]j, 2j]$ which are not covered. Let $R = \{r_1, r_2, \ldots, r_{k_s}\}$. Now for $s = 1, 2, \ldots$ we have $k_{s-1} = k_s - s\ell_s$. We may write this as

(2.3.2) $$\ell_s = \frac{k_s - k_{s-1}}{s} .$$

Note also that $k_o = 0$.

Consider the translations $A + i, A + (i + 1), \ldots,$ $A + (2j - 1)$ of A. Each translation covers at most s points of R. There are at most $2j - 1$ translations. The number of coverings of R therefore does not exceed $(2j - 1)s \leq 2js$. Also it is clear that each point r_m of R is covered exactly $A(r_m - i)$ times. Hence

$$A(r_m - i) + A(r_2 - i) \quad \ldots \quad + A(r_{k_s} - i) \leq 2js.$$

Since $r_m \geq j + 1$, we have $A(r_m - i) \geq A(j - i + 1)$. Hence $k_s A(j - i + 1) \leq 2js$, which we write as

(2.3.3) $$\frac{k_s}{s} \leq \frac{2j}{A(j - i + 1)} .$$

Let s_o be a positive integer not less than 2. The number of b's corresponding to values of $s < s_o$ is $\sum_{s=1}^{s_o-1} \ell_s$. The number of b's corresponding to values of $s \geq s_o$ does not exceed j/s_o since each choice of a b leads to the covering of at least s_o new points in $]j, 2j]$. Let ℓ be the total number of b's. Then

$$\ell \leq \sum_{s=1}^{s_o-1} \ell_s + \frac{j}{s_o} \leq \sum_{s=1}^{s_o} \ell_s + \frac{j}{s_o} .$$

Using (2.3.2) and (2.3.3), one easily obtains

$$\ell \leq \frac{2j}{A(j-i+1)} \sum_{s=1}^{s_o} \frac{1}{s} + \frac{j}{s_o} \leq \frac{c' \, j \log s_o}{A(j-i+1)} + \frac{j}{s_o}$$

for some suitable constant c'.

Choose $s_o = \left[\frac{A(j-i+1)}{\log A(j-i+1)} \right]$, where the square brackets denote the greatest integer function. It is clear that since $A(j-i+1) \geq 2$, $s_o \geq 2$. We have therefore

$$\ell \leq \frac{c' \, j \log [A(j-i+1)/\log A(j-i+1)]}{A(j-i+1)} + \frac{j}{[A(j-i+1)/\log A(j-i+1)]}$$

$$\leq \frac{c' \, j \, (\log A(j-i+1) - \log \log A(j-i+1))}{A(j-i+1)} + \frac{j}{\{A(j-i+1)/\log A(j-i+1)\} - 1}$$

$$= \frac{j \log A(j-i+1)}{A(j-i+1)} \left\{ c' - \frac{\log \log A(j-i+1)}{\log A(j-i+1)} + \frac{A(j-i+1)}{A(j-i+1) - \log A(j-i+1)} \right\}.$$

Noting that if $x \geq 2$, then $\frac{1}{2} \leq \frac{x}{x - \log x} \leq 2$ and $-1 \leq \frac{-\log \log x}{\log x} \leq 1$, we have

$$\ell \leq \frac{c \, j \log A(j-i+1)}{A(j-i+1)}$$

for some constant c. The lemma is established.

<u>Proof of Theorem 2.3.1</u>: For $m \geq r$, let $A(2^{m-1}) \geq 2$, $i = i(m) = 2^{m-1} + 1$ and $j = j(m) = 2^m$. Then $A(j-i+1) = A(2^{m-1}) \geq 2$. Hence i and j satisfy the hypothesis of the lemma. Let B_m be the set of b's in the interval $[i, 2j[\; = [2^{m-1} + 1, 2^{m+1}[$ constructed as in the lemma. Then $\{A + b;\ b \in B_m\}$ completely fills the interval $]j, 2j] =]2^m, 2^{m+1}]$. Denoting the number of b's in B_m by $\ell(m)$ we have, by the lemma,

$$\ell(m) \leq \frac{c' \, 2^{m-1} \log A(2^{m-1})}{A(2^{m-1})} .$$

Let $B = \bigcup_{m=r}^{\infty} B_m$. Let n be a positive integer. Then $B_m(n) = 0$ if $2^{m-1} \leq n$. We have therefore

$$B(n) \leq \sum_{\substack{2^{m-1} \leq n \\ m \geq r}} B_m(n) = \sum_{\substack{2^{m-1} \leq n \\ m \geq r}} \ell(m) < c' \sum_{\substack{2^{m-1} \leq n \\ m \geq r}} \frac{2^{m-1} \log A(2^{m-1})}{A(2^{m-1})}$$

$$= c' \left\{ \frac{2^{r-1} \log A(2^{r-1})}{A(2^{r-1})} + \sum_{\substack{2^{m-1} \leq n \\ m \geq r+1}} \frac{2^{m-1} \log A(2^{m-1})}{A(2^{m-1})} \right\}$$

$$\leq c' \left\{ \frac{2^{r-1} \log A(2^{r-1})}{A(2^{r-1})} + \sum_{\substack{2^{m-1} \leq n \\ m \geq r+1}} \sum_{t=1}^{2^{m-2}} \frac{2 \log A(2^{m-2} + t)}{A(2^{m-2} + t)} \right\}$$

$$\leq c' \left\{ \frac{2^{r-1} \log A(2^{r-1})}{A(2^{r-1})} + \sum_{k=2^{r-1}+1}^{n} \frac{2 \log A(k)}{A(k)} \right\}$$

$$\leq 2^r c' \sum_{k=2^{r-1}+1}^{n} \frac{\log A(k)}{A(k)} \leq c \sum_{k=1}^{n} \frac{\log A(k)}{A(k)}$$

which is (2.3.1).

We return to the conjecture of Erdös, namely, that given any infinite set A there exists a complementary set B of asymptotic density zero. Since $\frac{\log A(k)}{A(k)} \longrightarrow 0$ as $k \longrightarrow \infty$, i.e. since $\frac{\log A(k)}{A(k)} < \epsilon$ for $k > N = N(\epsilon)$, we have, by Theorem 2.3.1,

$$\frac{B(n)}{n} < \frac{c}{n}\sum_{k=1}^{N} \frac{\log A(k)}{A(k)} + \frac{c(n-N)\epsilon}{n} < \frac{c}{n}\sum_{k=1}^{N} \frac{\log A(k)}{A(k)} + c\epsilon.$$

Hence $\lim\limits_{n\to\infty} \frac{B(n)}{n} \leq c\epsilon$. This implies that $\lim\limits_{n\to\infty} \frac{B(n)}{n} = 0$.

Many other interesting results follow from the theorem of Lorentz. We present some of these here. If a particular set A is given then $A(k)$ can be determined explicitly. The right hand member of (2.3.1) can then be approximated by a definite integral, an upper bound for which can easily be obtained. Using this idea we prove

Theorem 2.3.2 There exists a set B satisfying $B(n) < \frac{c\, n \log\log n}{\log n}$ such that every sufficiently large positive integer can be expressed in the form $2^i + b$, where $b \in B$.

Proof: In Theorem 2.3.1, let $A = \{2^i;\ i = 0, 1, 2, \ldots\}$. Then there exists a complementary set B satisfying

$$B(n) < c_1 \sum_{k=1}^{n} \frac{\log A(k)}{A(k)} \leq c_1 \sum_{k=1}^{[\log_2 n]} \frac{2^k \log k}{k} < c_1 \int_1^{\log_2 n} \frac{2^x \log x}{x}\, dx.$$

It is easily verified that $\frac{2^x \log x}{x} < c_2 \frac{d}{dx}\left(\frac{2^x \log x}{x}\right)$ for some suitable constant c_2. Hence

$$B(n) < c_1 c_2 \frac{2^{\log_2 n} \log(\log_2 n)}{\log_2 n} = c_1 c_2 \log 2 \frac{n \log\log n}{\log n}\left\{1 - \frac{\log\log 2}{\log\log n}\right\}$$

$$< c\, \frac{n \log\log n}{\log n} .$$

It has been conjectured by Erdős [14] that there exists a set B satisfying $B(n) < cn/\log n$ such that every sufficiently large integer can be written in the form $2^i + b$. This conjecture remains unsettled.

Let A be the set of primes. Then, using Theorem 2.3.1 and Chebychev's theorem ($c_1 n/\log n < A(n) < c_2 n/\log n$ for suitable constants c_1 and c_2), it is easy to show that there exists a set B satisfying $c_1' \log n < B(n) < c_2'(\log n)^3$ such that every sufficiently large integer can be written in the form $p + b$, where p is a prime and $b \in B$. Erdös [14] showed that this result can be improved to $c_1' \log n < B(n) < c_2'(\log n)^2$.

If A is the set of squares, it follows from Theorem 2.3.1 that there exists a set B satisfying $B(n) < c\sqrt{n} \log n$ such that every sufficiently large integer can be expressed in the form $i^2 + b$. Erdös stated in [14] that this can be improved to $B(n) < c\sqrt{n}$ by taking B as the union of the sets of integers defined by $2^k < b < 2^k + 4.2^{k/2}$, $k = 1, 2, \ldots$. It is interesting to note, however, that if we take as our set B the union of the sets of integers defined by $2^k \leq b < 2^k + 2.2^{k/2}$, $k = 1, 2, \ldots$, the same result follows. In doing this the constant c is reduced considerably. Here we prove a more general result.

Theorem 2.3.3 There exists a set B satisfying $B(n) < c\, n^{1-1/s}$ such that every sufficiently large integer can be expressed in the form $i^s + b$.

Proof: We choose as our set B the integers in the intervals $2^k \leq b < 2^k + s.2^{k(1-1/s)}$, $k = 1, 2, \ldots$. Note that by setting $s = 2$, we get the result mentioned above. Let n be a positive integer and let $2^r < n \leq 2^{r+1}$. The number of b's not exceeding n is then

$$B(n) \le s \sum_{k=1}^{r} 2^{k(1-1/s)} + r = s.2^{(1-1/s)} \left\{ \frac{(2^{1-1/s})^r - 1}{2^{1-1/s} - 1} \right\} + r$$

$$\le (2^r)^{(1-1/s)} \left\{ \frac{s.2^{(1-1/s)}}{2^{1-1/s} - 1} + \frac{r}{(2^r)^{1-1/s}} \right\}.$$

Since $2^r \le n$, we have $r \le \log n/\log 2$. Hence

$$B(n) \le n^{1-1/s} \left\{ \frac{s.2^{(1-1/s)}}{2^{1-1/s} - 1} + \frac{\log n}{\log 2(2^r)^{1-1/s}} \right\}.$$

It is easy to show that $\dfrac{2^{1-1/s}}{2^{1-1/s} - 1} < \dfrac{7}{2}$ for all s, and that $\dfrac{\log n}{\log 2(2^r)^{1-1/s}} \longrightarrow 0$ as $n \longrightarrow \infty$. Hence, for n sufficiently large, $B(n) < 4s\, n^{1-1/s} = cn^{1-1/s}$.

We must next show that every sufficiently large integer can be written in the form $i^s + b$. Let, as before, $2^r < n \le 2^{r+1}$. We may then put $n = 2^r + m$, $0 < m \le 2^r$. Then $n - [\sqrt[s]{n - 2^r}\,]^s = 2^r + m - [\sqrt[s]{m}]^s \ge 2^r$. Also, using the fact that $(1 + a)^s \ge (1 + sa)$ for $a \ge -1$, we have

$$n - [\sqrt[s]{n - 2^r}]^s \le 2^r + m - (\sqrt[s]{m} - 1)^s = 2^r + m - m(1 - \frac{1}{\sqrt[s]{m}})^s$$

$$\le 2^r + m - m(1 - \frac{s}{\sqrt[s]{m}}) < 2^r + s.2^{r(1-1/s)}.$$

We have therefore

$$2^r \le n - [\sqrt[s]{n - 2^r}]^s < 2^r + s.2^{r(1-1/s)}$$

so that $n = i^s + b$, where $i = [\sqrt[s]{n - 2^r}]$ and $b \in B$.

We conclude this section with two other applications of the theorem of Lorentz.

__Theorem 2.3.2__ Let $n \geq \ell \geq 2$. If $a_1, a_2, \ldots, a_\ell$ is a set of incongruent residues modulo n, then there exists another set of residues $b_1, b_2, \ldots, b_k$ modulo n such that each residue modulo n can be written in the form $a_i + b_j$ and such that

$$k \leq \frac{c\, n \log \ell}{\ell}$$

for some constant c.

__Proof:__ We use Lemma 2.3.1. Let $a_1, a_2, \ldots, a_\ell$ be an arbitrary set of different positive integers not exceeding n. Choose $j = n$ and $i = 1$. Then $A(j - i + 1) = A(n) \geq \ell \geq 2$ so that the hypotheses of the lemma are satisfied. Hence there exists a set of integers $b_1, b_2, \ldots, b_k$ in $[1, 2n[$ such that all integers in $]n, 2n]$ are of the form $a_i + b_j$ and

$$k < \frac{c\, n \log \ell}{\ell} .$$

If we reduce the b_j and the $a_i + b_j$ modulo n, the theorem follows.

__Theorem 2.3.3__ If A is a set such that

$$\liminf_{n \to \infty} \frac{\log A(n)}{\log n} = \alpha > 0,$$

then there exists a complementary set B such that

$$\limsup_{n \to \infty} \frac{\log B(n)}{\log n} \leq 1 - \alpha .$$

Proof: Let ϵ be such that $\alpha > \epsilon > 0$. Then for all but a finite number of integers n we have

$$\frac{\log A(n)}{\log n} \geq \alpha - \epsilon \quad .$$

This implies that, except for finitely many n,

$$A(n) \geq n^{\alpha-\epsilon} \; .$$

By the theorem of Lorentz, we can find a complementary set B such that

$$B(n) \leq c \sum_{k=1}^{n} \frac{\log A(k)}{A(k)} \leq c \sum_{k=1}^{n} \frac{(\alpha - \epsilon) \log k}{k^{\alpha-\epsilon}} \; .$$

The sum on the right can be approximated by a definite integral and we obtain, after some straightforward computation,

$$\frac{\log B(n)}{\log n} \leq (1 - \alpha + \epsilon) + \frac{\log \log n}{\log n} + \frac{\log c(\alpha - \epsilon)}{\log n} \; .$$

Since ϵ is arbitrary, we have

$$\limsup_{n \to \infty} \frac{\log B(n)}{\log n} \leq 1 - \alpha \; .$$

We mention in passing that if A is the set of squares then one can find a complementary set B such that $B(n) < n^{1+2\epsilon/2}$ but this is not as good as either of the results mentioned earlier. Also, Theorem 2.3.3 does not apply to the case where A is the set of powers of 2 since we have in this case

$$\liminf_{n \to \infty} \frac{\log A(n)}{\log n} = 0 \; .$$

4. Hanani's Conjecture

Let A and B be infinite sets of positive integers such that every sufficiently large positive integer can be written in the form $a + b$, $a \in A$, $b \in B$. Then it is clear that

$$\limsup_{n \to \infty} \frac{A(n)\,B(n)}{n} \geq 1. \tag{2.4.1}$$

It was conjectured by Hanani that for any such sets A and B the following holds.

$$\limsup_{n \to \infty} \frac{A(n)\,B(n)}{n} > 1. \tag{2.4.2}$$

If one of the sets has positive lower asymptotic density then it is easy to show that (2.4.2) is true. In fact, we have

$$\limsup_{n \to \infty} \frac{A(n)\,B(n)}{n} = \infty .$$

If A is the set of squares, (2.4.2) holds. In fact, Moser [30] has given four different proofs that, in this case,

$$\liminf_{n \to \infty} \frac{A(n)\,B(n)}{n} \geq 1 + \epsilon.$$

The values obtained for ϵ are 0.06, 0.0013, 0.006 and 0.047. The methods used by Moser can be applied to sets other than the set of squares. These methods will be discussed in detail later in this chapter.

While Hanani's conjecture is unsettled, some results concerning it have recently been obtained by Narkiewicz [32]. We discuss these results next. The conjecture of Hanani can be stated in the following equivalent form. Let $f(n)$ be the number of representations of n in the form $a + b$, $a \in A$ and $b \in B$. If $f(n) \geq 1$ for all $n \geq n_0$

and if $\limsup_{n \to \infty} \frac{A(n)\,B(n)}{n} = 1$, then one of the sets A, B must be finite. The following theorem is due to Narkiewicz.

<u>Theorem 2.4.1</u> If $f(n) \geq 1$ for almost all integers* n and if $\limsup_{n \to \infty} \frac{A(n)\,B(n)}{n} \leq 1$, then

(a) $f(n) = 1$ for almost all integers n

(b) either $\lim_{n \to \infty} \frac{A(2n)}{A(n)} = 1$ or $\lim_{n \to \infty} \frac{B(2n)}{B(n)} = 1$.

<u>Proof</u>: (a) Let $M = \{m;\ f(m) \geq 2\}$. It is clear that

$$A(x)\,B(x) \geq x + M(x) + o(x).$$

Hence

$$\frac{A(x)\,B(x)}{x} \geq 1 + \frac{1}{x}\,(M(x) + o(x)).$$

Since $\limsup_{x \to \infty} \frac{A(x)\,B(x)}{x} \leq 1$, it follows that $M(x) = o(x)$. This implies that M has asymptotic density zero and hence that $f(n) = 1$ for almost all integers n.

(b) Let $g(x, t) = \sum_{\substack{t = a+b \\ a \leq x,\ b \leq x}} 1$ and let $h(x) = \sum_{t > x} g(x, t)$. Then

$$A(x)\,B(x) = \sum_{t \leq 2x} g(x, t) = h(x) + \sum_{t \leq x} g(x, t)\ .$$

We write this as

$$0 \leq h(x) = A(x)\,B(x) - \sum_{t \leq x} g(x, t).$$

---

* A set is said to contain almost all integers if it has asymptotic density 1.

But $A(x)\, B(x) = x + o(x)$ and $\sum_{t \le x} g(x, t) = x + o(x)$. Hence

$$(2.4.3) \qquad 0 \le h(x) = o(x).$$

Loosely speaking, (2.4.3) states that the a's and b's not exceeding x do not yield many sums a + b exceeding x.

We consider the functions $p(x) = A(x/2)/A(x)$ and $q(x) = B(x/2)/B(x)$ and show that these cannot have limit points other than 1/2 and 1 as $x \to \infty$. Note that if $x/2 < a \le x$ and $x/2 < b \le x$, then $a + b > x$. Hence

$$(2.4.4) \qquad h(x) \ge (A(x) - A(x/2))(B(x) - B(x/2)) \ge 0.$$

We also have

$$\begin{aligned}(2.4.5) \quad (A(x) - A(x/2))(B(x) - B(x/2)) &= A(x)\, B(x) - A(x)\, B(x/2) - A(x/2)\, B(x) + A(x/2)\, B(x/2) \\ &= x + o(x) - A(x)\, B(x/2) - A(x/2)\, B(x) + x/2 + o(x) \\ &= 3x/2 - A(x)\, B(x/2) - A(x/2)\, B(x) + o(x).\end{aligned}$$

From (2.4.3), (2.4.4) and (2.4.5) it follows that

$$\lim_{x \to \infty} \frac{A(x)\, B(x/2) + A(x/2)\, B(x)}{x} = \frac{3}{2}.$$

This can be written in the following form:

$$\lim_{x \to \infty} \frac{A(x)}{2A(x/2)} \left\{\frac{A(x/2)\, B(x/2)}{x/2}\right\} + \frac{A(x/2)}{A(x)} \left\{\frac{A(x)\, B(x)}{x}\right\} = \frac{3}{2}.$$

Hence $\displaystyle\lim_{x \to \infty} \frac{A(x)}{2A(x/2)} + \frac{A(x/2)}{A(x)} = \frac{3}{2}.$

By the definition of $p(x)$ we have

$$\lim_{x \to \infty} \frac{1}{2p(x)} + p(x) = \frac{3}{2}.$$

Let z be one of the limit points of $p(x)$ as $x \to \infty$. Then there exists a sequence of integers $\{x_i\}$ such that $\lim_{i \to \infty} p(x_i) = z$. z must satisfy the equation $\frac{1}{2z} + z = \frac{3}{2}$. We have therefore $z = 1$ or $z = \frac{1}{2}$. Similar statements can be made about $q(x)$.

Now $p(x)\, q(x) = A(x/2)\, B(x/2)/A(x)\, B(x) \to \frac{1}{2}$ as $x \to \infty$. Hence if $p(x_i) \to \frac{1}{2}$ then $q(x_i) \to 1$ and if $q(x_i) \to \frac{1}{2}$ then $p(x_i) \to 1$. We assume that $p(x_i) \to 1$. Our aim is to show that $p(x) \to 1$. To accomplish this we need the following lemma.

<u>Lemma 2.4.1</u> Let $\{t_k\}$ be a monotone increasing sequence of positive integers such that $p(t_k) \to 1$ as $k \to \infty$. Then $\lim_{k \to \infty} \frac{A(t_k/4)}{A(t_k)} = 1$.

<u>Proof of the Lemma</u>: We have

$$(2.4.6) \qquad h(x) \geq (A(x) - A(x/4))(B(x) - B(3x/4)).$$

Also

$$(2.4.7) \qquad (A(x) - A(x/4))(B(x) - B(3x/4))$$
$$= x - B(x)\, A(x/4) - B(3x/4)\, A(x) + B(3x/4)\, A(x/4) + o(x).$$

From (2.4.3), (2.4.6) and (2.4.7) it follows that

$$\lim_{x \to \infty} \frac{B(x)\, A(x/4) + B(3x/4)\, A(x) - B(3x/4)\, A(x/4)}{x} = 1.$$

This can be written as

$$\lim_{x \to \infty} \left[\frac{A(x/4)}{A(x)} \left\{ \frac{A(x)\ B(x)}{x} \right\} + \frac{3A(x)}{4A(3x/4)} \left\{ \frac{A(3x/4)\ B(3x/4)}{3x/4} \right\} - \frac{3A(x/4)}{4A(3x/4)} \left\{ \frac{A(3x/4)\ B(3x/4)}{3x/4} \right\} \right] = 1.$$

Hence

$$\lim_{x \to \infty} \left\{ \frac{A(x/4)}{A(x)} + \frac{3A(x)}{4A(3x/4)} - \frac{3A(x/4)}{4A(3x/4)} \right\} = 1. \tag{2.4.8}$$

Now $$1 \leq \frac{A(t_k)}{A(3t_k/4)} \leq \frac{A(t_k)}{A(t_k/2)} = \frac{1}{p(t_k)} \longrightarrow 1.$$

Hence

$$\lim_{k \to \infty} \frac{A(t_k)}{A(3t_k/4)} = 1. \tag{2.4.9}$$

Putting $x = t_k$ in (2.4.8) and using (2.4.9) we have

$$1 = \lim_{k \to \infty} \left\{ \frac{A(t_k/4)}{A(t_k)} + \frac{3}{4} \frac{A(t_k)}{A(3t_k/4)} - \frac{3A(t_k/4)\ A(t_k)}{4A(t_k)\ A(3t_k/4)} \right\}$$

$$= \lim_{k \to \infty} \frac{A(t_k/4)}{A(t_k)} = 1, \text{ as asserted.}$$

We proceed with the proof of the theorem. Let $\{y_n\}$ be a monotone increasing sequence of positive integers. Let $S = \{x;\ |1/p(x) - 1| < 1/4\}$. Since $p(x_i) \longrightarrow 1$, it follows that S is an infinite set. Let $u_n = \inf_{\substack{x \geq y_n \\ x \in S}} x$. It is clear that $u_n \in S$. We therefore have

$$\left| \frac{A(u_n)}{A(u_n/2)} - 1 \right| < \frac{1}{4}.$$

This implies that a subsequence $\{u_{n_k}\}$ of $\{u_n\}$ for which $p(u_{n_k}) \to \frac{1}{2}$ does not exist. Hence $p(u_n) \to 1$.

By the lemma $\lim_{n \to \infty} \frac{A(u_n)}{A(u_n/4)} = 1$. Hence

$$(2.4.10) \qquad \lim_{n \to \infty} \frac{A(u_n/2)}{A(u_n/4)} = \lim_{n \to \infty} \frac{A(u_n/2)}{A(u_n)} \frac{A(u_n)}{A(u_n/4)} = 1.$$

We assert that for n sufficiently large, $u_n/2 \leq y_n$. To see this, suppose that for an infinite sequence $\{n_k\}$ we have $u_{n_k}/2 > y_{n_k}$.

Then $u_{n_k}/2 \notin S$ and $\left| \frac{A(u_{n_k}/2)}{A(u_{n_k}/4)} - 1 \right| \geq \frac{1}{4}$ which contradicts (2.4.10).

Hence, when n is sufficiently large, we have

$$u_n/4 \leq y_n/2 \leq u_n/2 \leq y_n \leq u_n .$$

Hence

$$A(u_n/4) \leq A(y_n/2) \leq A(u_n/2) \leq A(y_n) \leq A(u_n).$$

It follows that

$$\lim_{n \to \infty} \frac{A(y_n)}{A(y_n/2)} = 1 .$$

Since the sequence $\{y_n\}$ is arbitrary, we have $\lim_{x \to \infty} p(x) = 1$. The theorem follows.

It is important to note that both the hypothesis and conclusion of Narkiewicz's theorem are weaker than those of Hanani's conjecture.

5. Some Results of Moser on the Addition of Two Sets of Integers

Let B be a set of non-negative integers* with the property that every positive integer can be written in the form $k^2 + b$, $b \in B$. It is clear that $B(n) \geq \sqrt{n}$. Moser has shown, using four different methods, that $B(n) \geq \sqrt{n}(1 + \epsilon)$. Each method gives an explicit value for $\epsilon > 0$.

Theorem 2.5.1 $B(n) \geq 1.06 \sqrt{n}$ for n sufficiently large.

Proof: Let $\{a_1, a_2, \dots, a_k\}$ and $\{b_1, b_2, \dots, b_k\}$ be two sets of numbers. It is easily verified that

$$(2.5.1) \qquad \frac{1}{k}\sum_{i=1}^{k} a_i + \frac{1}{\ell}\sum_{j=1}^{\ell} b_j = \frac{1}{k\ell}\sum_{i=1}^{k}\sum_{j=1}^{\ell}(a_i + b_j) .$$

We may choose $k = [\sqrt{n}]$, $a_i = i^2$, $\ell = B(n)$, and the b_j as the elements of B not exceeding n. Then

$$(2.5.2) \qquad \frac{1}{k}\sum_{i=1}^{k} a_i = \frac{1}{[\sqrt{n}]}\sum_{i=1}^{[\sqrt{n}]} i^2 = \frac{2\,[\sqrt{n}]^2 + 3[\sqrt{n}] + 1}{6} < 0.34\, n$$

for n sufficiently large. Since we are assuming that the numbers $1, 2, \dots, n$ are of the form $a_i + b_j$, the right hand side of (2.5.1) is at least

$$\frac{1}{k\ell}(1 + 2 + \dots + n) = \frac{n(n+1)}{2\,[\sqrt{n}]\,\ell} \geq \frac{n^{3/2}}{2\ell} .$$

This, together with (2.5.1) and (2.5.2), implies

$$(2.5.3) \qquad \sum_{j=1}^{\ell} b_j > \frac{1}{2} n^{3/2} - 0.34\, n\ell.$$

---

* Here we are departing from our convention that capital letters denote sets of positive integers.

Now for each b_j and every i such that $b - b_j < i^2 \leq n$ we have a number of the form $i^2 + b_j$ which exceeds n, i.e. for each j we have $[\sqrt{n}] - [\sqrt{n - b_j}]$ numbers of the form $i^2 + b_j$ exceeding n. Hence

$$[\sqrt{n}]\ell \geq n + \sum_{j=1}^{\ell} ([\sqrt{n}] - [\sqrt{n - b_j}]) \geq n + \sum_{j=1}^{\ell} (\sqrt{n} - \sqrt{n - b_j}) - \ell .$$

It is easily verified that for $x \geq 0$ and $t \geq 0$ the following inequality holds.

$$\sqrt{x + t} - \sqrt{x} \geq t / 2\sqrt{x + t}$$

Setting $x = n - b_j$ and $t = b_j$, we have

$$\sqrt{n} - \sqrt{n - b_j} \geq b_j / 2\sqrt{n} .$$

Hence

$$[\sqrt{n}]\ell \geq n + \frac{1}{2\sqrt{n}} \sum_{j=1}^{\ell} b_j - \ell .$$

We may write this as

$$\sum_{j=1}^{\ell} b_j \leq 2n\ell - 2n^{3/2} + 2\sqrt{n}\,\ell . \tag{2.5.4}$$

Combining (2.5.3) and (2.5.4) we have

$$0.5\, n^{3/2} - 0.34\, n\ell < 2n\ell - 2n^{3/2} + 2\sqrt{n}\,\ell .$$

This reduces to

$$(2.34 + \frac{2}{\sqrt{n}})\ell > 2.50\sqrt{n} .$$

For n sufficiently large this implies

$$\ell > 1.06\sqrt{n} .$$

Remark: Formula (2.5.1) is simply the statement of the fact that the sum of the means of two distributions is the mean of the distribution of the sum. In view of this, the method used in Theorem 2.5.1 may well be called the "method of means". The method of means can be applied to other sequences; for example, the sequence of m th powers. It will fail, however, if the a's are such that no estimate of the number of $a_i + b_j$ exceeding n can be obtained. It will also fail if the mean value of the a's is nearly zero or $\frac{n}{2}$, i.e. if no estimate of the form (2.5.2) can be obtained.

We discuss next the second of Moser's methods, called the method of variances. Let, as before, A and B be sets of non-negative integers with the property that every positive integer can be expressed in the form $a + b$, $a \in A$, $b \in B$. Let n be a positive integer and let $\{a_1, a_2, \ldots, a_k\}$, $\{b_1, b_2, \ldots, b_\ell\}$ be the elements of A and B which do not exceed n. Let

$$\bar{a} = \frac{1}{k}\sum_{i=1}^{k} a_i \quad \text{and} \quad \bar{b} = \frac{1}{\ell}\sum_{j=1}^{\ell} b_j .$$

Also let

$$V(A) = \frac{1}{k}\sum_{i=1}^{k} (a_i - \bar{a})^2 \quad \text{and} \quad V(B) = \frac{1}{\ell}\sum_{j=1}^{\ell} (b_j - \bar{b})^2 .$$

We prove the following theorem.

<u>Theorem 2.5.2</u> If $V(A) \geq n^2(1/12 + \alpha)$ where $\alpha > 0$, then $k\ell > n(1 + \alpha/4)$.

The theorem depends on the following lemma.

<u>Lemma 2.5.1</u> Let r be a positive number and let $c_1, c_2, \ldots, c_s, c_{s+1}, \ldots, c_{s+t}$ be positive numbers not exceeding r. Let $\bar{c} = \frac{1}{s}\sum_{i=1}^{s} c_i$ and $\bar{c}' = \frac{1}{s+t}\sum_{i=1}^{s+t} c_i$. Then $\frac{1}{s+t}\sum_{i=1}^{s+t}(c_i - \bar{c}')^2 \leq \frac{1}{s}\sum_{i=1}^{s}(c_i - \bar{c})^2 + \frac{tr^2}{s}$.

<u>Proof</u>: It is clear that $\frac{1}{s+t}\sum_{i=1}^{s+t}(c_i - x)^2$ is minimized at $x = \bar{c}'$. Hence

$$\frac{1}{s+t}\sum_{i=1}^{s+t}(c_i - \bar{c}')^2 \leq \frac{1}{s+t}\sum_{i=1}^{s+t}(c_i - \bar{c})^2$$

$$= \frac{1}{s+t}\sum_{i=1}^{s}(c_i - \bar{c})^2 + \frac{1}{s+t}\sum_{i=s+1}^{s+t}(c_i - \bar{c})^2$$

$$\leq \frac{1}{s}\sum_{i=1}^{s}(c_i - \bar{c})^2 + \frac{1}{s}\sum_{i=s+1}^{s+t}c_i^2 \leq \frac{1}{s}\sum_{i=1}^{s}(c_i - \bar{c})^2 + \frac{tr^2}{s}.$$

We proceed with the proof of the theorem. It is easy to verify that

$$(2.5.5) \quad \frac{1}{k}\sum_{i=1}^{k}(a_i - \bar{a})^2 + \frac{1}{\ell}\sum_{j=1}^{\ell}(b_i - \bar{b})^2$$

$$= \frac{1}{k\ell}\sum_{i=1}^{k}\sum_{j=1}^{\ell}(a_i + b_j - \bar{a} - \bar{b})^2 .$$

Now the $a_i + b_j$ represent the numbers $1, 2, \ldots, n$ together with $k\ell - n$ other numbers each not exceeding $2n$. In the above lemma we may let $r = 2n$, $s = n$, $s + t = k\ell$, $c_m = m$ for $m = 1, 2, \ldots, n$, and c_m = one of the remaining $k\ell - n$ numbers of the form $a_i + b_j$ for $m > n$. Then

$$\frac{1}{k\ell}\sum_{i=1}^{k}\sum_{j=1}^{\ell}(a_i + b_j - \bar{a} - \bar{b})^2 \leq \frac{1}{n}\sum_{m=1}^{n}\left(m - \frac{1}{n}\sum_{j=1}^{n} j\right)^2 + (k\ell - n)4n .$$

This simplifies to

$$(2.5.6)\quad \frac{1}{k\ell}\sum_{i=1}^{k}\sum_{j=1}^{\ell}(a_i + b_j - \bar{a} - \bar{b})^2 \leq \frac{n^2 - 1}{12} + 4n(k\ell - n) .$$

Using (2.5.5) and (2.5.6) and noting that

$$\frac{1}{\ell}\sum_{j=1}^{\ell}(b_i - \bar{b})^2 \geq 0$$

we have

$$n^2(1/12 + \alpha) \leq V(A) = \frac{1}{k}\sum_{i=1}^{k}(a_i - \bar{a})^2$$

$$\leq \frac{1}{k\ell}\sum_{i=1}^{k}\sum_{j=1}^{\ell}(a_i + b_j - \bar{a} - \bar{b})^2 \leq \frac{n^2}{12} + 4n(k\ell - n).$$

The extreme members of this inequality yield

$$k\ell > n(1 + \alpha/4),$$

as required.

Equation (2.5.5) is in fact a special case of the well-known theorem that the variance of the sum of two independent distributions is equal to the sum of the variances of the two distributions, hence the name variance method. If A is the set of squares, then it is easy to show that $V(A) \sim \frac{4}{45} n^2 = n^2(\frac{1}{12} + \frac{1}{180})$. This implies that $[\sqrt{n}]\ell > n(1 + \frac{1}{720})$ which in turn implies $\ell > \sqrt{n}(1.0013)$. We note also that this method does not apply when A is the set of m th powers, $m \geq 3$. The reason is that the variance of the cubes or higher powers in $[1, n]$ is less than $n^2/12$.

We discuss next a method which is analytical in nature. Let A be the set of squares. That every integer in $[1, n]$ can be expressed in the form $t^2 + b_j$ is expressed analytically by the following identity.

$$(2.5.7) \quad \sum_{t=1}^{[\sqrt{n}]} z^{t^2} \sum_{j=1}^{\ell} z^{b_j} = \sum_{t=1}^{n} z^t + \sum_{j=1}^{2n} f(j) z^j .$$

$f(j) \geq 0$ is also defined by (2.5.7). If we put $z = 1$ in (2.5.7) we get the trivial result $[\sqrt{n}]\ell \geq n$. We shall show that for some value of z on the unit circle, $\left|\sum_{j=1}^{2n} f(j) z^j\right|$ is large. Let $z = e^{\pi i/n}$. With this value of z, we have

$$(2.5.8) \quad \left|\sum_{t=1}^{n} z^t\right| = \left|\sum_{t=1}^{n} e^{t\pi i/n}\right| \simeq \left|\sum_{t=0}^{n} \cos\frac{t\pi}{n} + i\sum_{t=0}^{n} \sin\frac{t\pi}{n}\right|$$

$$\simeq \left|\int_0^n \cos\frac{\pi x}{n}\,dx + i\int_0^n \sin\frac{\pi x}{n}\,dx\right| = \frac{2n}{\pi} .$$

Also
$$\left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2}\right|^2 = \left(\sum_{t=1}^{[\sqrt{n}]} \cos\frac{\pi t^2}{n}\right)^2 + \left(\sum_{t=1}^{[\sqrt{n}]} \sin\frac{\pi t^2}{n}\right)^2$$

$$\simeq \left(\int_o^{[\sqrt{n}]} \cos\frac{\pi x^2}{n}\, dx\right)^2 + \left(\int_o^{[\sqrt{n}]} \sin\frac{\pi x^2}{n}\, dx\right)^2$$

$$\simeq \left(\sqrt{n}\int_o^1 \cos\pi y^2\, dy\right)^2 + \left(\sqrt{n}\int_o^1 \sin\pi y^2\, dy\right)^2,$$

where we have put $x = \sqrt{n}\, y$. These integrals may be evaluated numerically by means of tables [43] to yield, for sufficiently large n,

(2.5.9)
$$\left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2}\right| < 0.62\sqrt{n} .$$

Also we have

(2.5.10)
$$\left|\sum_{j=1}^{\ell} z^{b_j}\right| \leq \ell .$$

From (2.5.9) and (2.5.10) we get

(2.5.11)
$$\left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2} \sum_{j=1}^{\ell} z^{b_j}\right| < 0.62\sqrt{n}\,\ell .$$

Hence

$$(2.5.12)\quad \sum_{j=1}^{2n} f(j) \geq \left|\sum_{j=1}^{2n} f(j)\, z^j\right| = \left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2} \sum_{j=1}^{\ell} z^{b_j} - \sum_{j=1}^{n} z^t\right|$$

$$\geq - \left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2}\right| \left|\sum_{j=1}^{\ell} z^{b_j}\right| + \left|\sum_{t=1}^{n} z^t\right|$$

$$> \frac{2n}{\pi} - 0.62\sqrt{n}\,\ell\ .$$

Putting $z = 1$ in (2.5.7) we get

$$[\sqrt{n}]\ell \geq n + \sum_{j=1}^{2n} f(j)\ .$$

This with (2.5.12) yields

$$[\sqrt{n}]\ell \geq n + \frac{2n}{\pi} - 0.62\sqrt{n}\,\ell.$$

For n sufficiently large this implies

$$(2.5.13)\qquad \ell > 1.006\sqrt{n}.$$

Choose $z = e^{2\pi i/n}$. Then $\sum_{t=1}^{n} z^t = 0$. Hence for this value of z we have

$$(2.5.14)\qquad \left|\sum_{j=1}^{2n} f(j)\, z^j\right| = \left|\sum_{j=1}^{\ell} z^{b_j}\right| \left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2}\right|$$

We may use tables of Fresnel's integrals to show that for n sufficiently large

$$(2.5.15)\qquad \left|\sum_{t=1}^{[\sqrt{n}]} z^{t^2}\right| > 0.29\sqrt{n}\ .$$

Suppose that at least $3/4$ of the b's are contained in $[1, n/4]$. For each b_j in the interval $[1, n/4]$, the projection of the vector z^{b_j} on the line $\theta = \pi/4$ is at least $1/\sqrt{2}$. For each b_j not in the interval $[1, n/4]$, the projection on the line $\theta = \pi/4$ is greater than or equal to -1. Hence

$$(2.5.16) \qquad \left| \sum_{j=1}^{\ell} z^{b_j} \right| \geq \left(\frac{3}{4\sqrt{2}} - \frac{1}{4}\right)\ell > 0.275\,\ell .$$

From (2.5.14), (2.5.15) and (2.5.16) we get

$$\left| \sum_{j=1}^{2n} f(j)\, z^j \right| > (0.275\,\ell)\,(0.29\sqrt{n}) .$$

This implies

$$\sum_{j=1}^{2n} f(j) > 0.079\,\ell\sqrt{n} .$$

Putting $z = 1$ in (2.5.7) we get

$$[\sqrt{n}]\,\ell = n + \sum_{j=1}^{2n} f(j) > n + 0.079\,\ell\sqrt{n}.$$

This implies

$$(2.5.17) \qquad \ell > 1.09\sqrt{n} .$$

We must also consider the case when at least $1/4$ of the b's are in the interval $[3n/4, n]$. The number of squares in this interval is $[\sqrt{n}] - [\sqrt{3n/4}] > 0.268\sqrt{n}$ for n sufficiently large. Hence the sums $t^2 + b_j$ where t^2 and b_j are in $[3n/4, n]$ represent at least $\frac{\ell}{4}(0.268\sqrt{n})$ numbers exceeding n. This implies

$$[\sqrt{n}]\,\ell \;\geq\; n + 0.067\,\sqrt{n}\,\ell$$

which in turn implies

$$\ell > 1.046\,\sqrt{n} \quad . \tag{2.5.18}$$

Note that (2.5.18) holds in any case.

CHAPTER III

SOME RELATED TOPICS

1. A Theorem of Erdős and Fuchs

Let $A = \{a_1 < a_2 < \dots\}$ be an infinite sequence of positive integers. Let $f(n)$ be the number of solutions of $n = a_i + a_j$ where $a_i + a_j$ counts once if $i = j$ and twice if $i \neq j$. Erdős and Turán [12] proved, using a considerable amount of function theory, that $f(n)$ cannot be constant from some point on. However, Dirac [9] observed that this is trivial for if $n = 2a_i$, then $f(n)$ is odd but if n is not of this form, then $f(n)$ is even. Denote by $f'(n)$ the number of solutions of $n = a_i + a_j$ where each solution counts once. Dirac [9] gave a very elegant proof that $f'(n)$ cannot be constant from some point on. His argument goes as follows. Assume that for some positive integer c, $f'(m + 1) = f'(m + 2) = f'(m + 3) = \dots = c$. Then we have

$$\frac{1}{2}\left\{\left(\sum_{k=1}^{\infty} z^{a_k}\right)^2 + \sum_{k=1}^{\infty} z^{2a_k}\right\} = \sum_{n=0}^{\infty} f'(n)\, z^n$$

$$= P_m(z) + \frac{c\, z^{m+1}}{(1 - z)}$$

where $P_m(z)$ is a polynomial in z of degree not exceeding m. Let $z \longrightarrow -1$. Then $P_m(z) + \frac{c\, z^{m+1}}{1 - z}$ remains bounded whereas $\frac{1}{2}\left\{\left(\sum_{k=1}^{\infty} z^{a_k}\right)^2 + \sum_{k=1}^{\infty} z^{2a_k}\right\} \longrightarrow \infty$. It follows that $f'(n)$ is not constant from some point on.

Let $f''(n)$ be the number of solutions of $n = a_i + a_j$ where only the solutions with $i \neq j$ are counted. Dirac [9] conjectured that $f''(n)$ is not constant from some point on but was unable to prove it. The conjecture was proved by Erdös and Fuchs [17]. Actually, they proved much more than this and we discuss their results next.

Let $f(n)$ be the number of solutions of $n = a_i + b_j$ and let $f(n)$ have any one of the three interpretations discussed above. We prove the following theorem.

Theorem 3.1.1 Let $r(n) = \sum_{k=0}^{n} f(k)$. Then $r(n) = cn + o(n^{1/4}/\sqrt{\log n})$ is false for all $c > 0$.

Remark Before entering into the details of the proof we show that Theorem 3.1.1 implies that $f(n)$ is not a constant from some point on. We assume the contrary, i.e. that $f(n) = m$ for all $n \geq n_o$. Then

$$\left|\left(\sum_{k=0}^{n} f(k) - mn\right)\frac{\sqrt{\log n}}{n^{1/4}}\right| = \left|\left(\sum_{k=0}^{n_o-1} f(k) - (n_o + 1)m\right)\frac{\sqrt{\log n}}{n^{1/4}}\right| \to 0$$

as $n \to \infty$. This contradicts the conclusion of the theorem with $c = m$.

In order to prove the theorem we need the following lemma.

Lemma 3.1.1 Let $\varphi(z) = \sum_{n=0}^{\infty} b_n z^n$ converge for $|z| < 1$, and suppose the b_n are non-negative real numbers. Then for $0 < \alpha \leq \pi$, $z = re^{i\theta}$, $o < r < 1$ we have

$$\int_{-\alpha}^{\alpha} |\varphi\,(z)|^2\, d\theta \;\geq\; \frac{\alpha}{3\pi}\int_{-\pi}^{\pi} |\varphi(z)|^2\, d\theta\,. \tag{3.1.1}$$

Proof: Consider the function $h(\theta)$ defined by

$$\begin{aligned} h(\theta) &= 1 - \left|\frac{\theta}{\alpha}\right| && \text{if } |\theta| < \alpha \\ h(\theta) &= 0 && \text{if } \alpha \leq |\theta| \leq \pi\,. \end{aligned} \tag{3.1.2}$$

Let the Fourier series for $h(\theta)$ be

$$h(\theta) = a_o + \sum_{m=1}^{\infty} (a_m \cos m\theta + b_m \sin m\theta)\,. \tag{3.1.3}$$

We find by the usual method of computing Fourier coefficients that

$$a_o = \frac{\alpha}{2\pi}\,, \quad a_m = \frac{2(1 - \cos \alpha m)}{\pi\,\alpha\, m^2} \quad \text{for } m \geq 1, \quad \text{and } b_m = 0.$$

Hence we obtain from (3.1.3)

$$h(\theta) = \sum_{k=-\infty}^{\infty} c_k e^{ik\theta} \tag{3.1.4}$$

where $c_k = \dfrac{1 - \cos \alpha k}{\pi\,\alpha\, k^2}$ for $k \neq 0$ and $c_o = \dfrac{\alpha}{2\pi}$.

It is easy to check that for $z = re^{i\theta}$,

$$|\varphi(z)|^2 = \sum_{n,\ell=0}^{\infty} b_n\, b_\ell\, r^{n+\ell} \cos(n - \ell)\theta, \tag{3.1.5}$$

From (3.1.4) and (3.1.5) we get

$$h^2(\theta)\; |\varphi(z)|^2 = \sum_{\substack{k,m=-\infty \\ n,\ell=0}}^{\infty} c_k c_m e^{i(k+m)\theta}\; b_n b_\ell r^{n+\ell} \cos(n - \ell)\theta\,.$$

Noting that

$$\int_{-\pi}^{\pi} e^{i(k+m)\theta} \cos(n - \ell)\theta \, d\theta = \begin{cases} 0 \text{ if } k + m \neq \pm(n - \ell) \\ \pi \text{ if } k + m = \pm(n - \ell) \end{cases}$$

we get,

$$(3.1.6) \quad \int_{-\pi}^{\pi} h^2(\theta)\, |\varphi(z)|^2 \, d\theta = 2\pi \sum_{\nu=-\infty}^{\infty} \Big(\sum_{k+\ell=\nu} c_k b_\ell r^\ell \Big)^2$$

$$\geq 2\pi \sum_{\nu=-\infty}^{\infty} \sum_{k+\ell=\nu} c_k^{\,2}\, b_\ell^{\,2}\, r^{2\ell} = 2\pi \sum_{k=-\infty}^{\infty} c_k^{\,2} \sum_{\ell=0}^{\infty} b_\ell^{\,2}\, r^{2\ell}.$$

Now

$$h^2(\theta) = \sum_{k,\ell=-\infty}^{\infty} c_k\, c_\ell\, e^{i(k+\ell)\theta}.$$

Since

$$\int_{-\pi}^{\pi} e^{i(k+\ell)\theta} \, d\theta = \begin{cases} 0 & \text{if } k \neq -\ell \\ 2\pi & \text{if } k = -\ell \end{cases},$$

we have

$$(3.1.7) \quad \int_{-\pi}^{\pi} h^2(\theta) \, d\theta = 2\pi \sum_{k=-\infty}^{\infty} c_k^{\,2} .$$

Noting that

$$\int_{-\pi}^{\pi} \cos\,(n - \ell)\theta \, d\theta = \begin{cases} 0 & \text{if } n \neq \ell \\ 2\pi & \text{if } n = \ell \end{cases},$$

we have, from (3.1.5),

$$(3.1.8) \quad \int_{-\pi}^{\pi} |\varphi(z)|^2 \, d\theta = 2\pi \sum_{\ell=0}^{\infty} b_\ell^{\,2}\, r^{2\ell} .$$

From (3.1.6), (3.1.7) and (3.1.8) we get

$$(3.1.9) \quad \int_{-\pi}^{\pi} h^2(\theta)\ |\varphi(z)|^2\ d\theta \ \geq\ \frac{1}{2\pi} \int_{-\pi}^{\pi} h^2(\theta)\ d\theta \int_{-\pi}^{\pi} |\varphi(z)|^2\ d\theta\ .$$

By (3.1.2)

$$h^2(\theta) = 1 - 2\left|\frac{\theta}{\alpha}\right| + \frac{\theta^2}{\alpha^2}\ , \text{if } |\theta| < \alpha$$

and

$$h^2(\theta) = 0 \qquad , \text{if } \alpha \leq |\theta| \leq \pi.$$

Hence

$$\int_{-\pi}^{\pi} h^2(\theta)\ d\theta = \int_{-\alpha}^{\alpha} \left(1 - 2\left|\frac{\theta}{\alpha}\right| + \frac{\theta^2}{\alpha^2}\right) d\theta = \frac{2\alpha}{3}\ .$$

This, together with (3.1.9), gives

$$\int_{-\pi}^{\pi} h^2(\theta)\ |\varphi(z)|^2\ d\theta \ \geq\ \frac{\alpha}{3\pi} \int_{-\pi}^{\pi} |\varphi(z)|^2\ d\theta\ .$$

Now when $|\theta| < \alpha$, $h^2(\theta) \leq 1$, and $h^2(\theta) = 0$ otherwise. Hence

$$\int_{-\alpha}^{\alpha} |\varphi(z)|^2\ d\theta \ \geq\ \int_{-\pi}^{\pi} h^2(\theta)\ |\varphi(z)|^2\ d\theta \ \geq\ \frac{\alpha}{3\pi} \int_{-\pi}^{\pi} |\varphi(z)|^2\ d\theta.$$

The lemma is established.

We proceed with the proof of Theorem 3.1.1. Recall that $f(n)$, which is the number of solutions of $a_i + a_j = n$, can be interpreted in three different ways:

(a) count a solution once if $i = j$ and twice if $i \neq j$

(b) count a solution once if $i = j$ and once if $i \neq j$

(c) count a solution once if $i \neq j$ and not at all if $i = j$.

If we set $g(z) = \sum_{k=1}^{\infty} z^{a_k}$, the corresponding generating functions are (a) $g^2(z)$, (b) $\frac{1}{2}(g^2(z) + g(z^2))$, (c) $\frac{1}{2}(g^2(z) - g(z^2))$. Let $H(z)$ be any one of the three generating functions. Then

$$H(z) = \sum_{n=0}^{\infty} f(n)\, z^n$$

and

$$(1 - z)^{-1} H(z) = \sum_{n=0}^{\infty} r(n)\, z^n .$$

We must show that

$$(1 - z)^{-1} H(z) = c \sum_{n=0}^{\infty} n\, z^n + h(z),$$

where $h(z) = \sum_{n=0}^{\infty} v_n z^n$ and $v_n = o(n^{1/4}/\sqrt{\log n}\,)$, is false for all $c > 0$. Since $\sum_{n=0}^{\infty} n\, z^n = z(1 - z)^{-2}$, we have to show that

$$(3.1.10) \qquad (1 - z)^{-1} H(z) = cz(1 - z)^{-2} + h(z)$$

is false for all $c > 0$. Assume that (3.1.10) can hold. Let $1/2 < r < 1$, $z = re^{i\theta}$, $1 - r < \alpha < \pi$. Then

$$\int_{-\alpha}^{\alpha} |H(z)|\, d\theta = \int_{-\alpha}^{\alpha} |cz(1 - z)^{-1} + h(z)\,(1 - z)|\, d\theta$$

$$\leq c \int_{-\alpha}^{\alpha} |z|\, |(1 - z)^{-1}|\, d\theta + \int_{-\alpha}^{\alpha} |h(z)|\, |1 - z|\, d\theta .$$

Noting that $|z| < 1$ and $\alpha < \pi$ we have

$$(3.1.11) \quad \int_{-\alpha}^{\alpha} |H(z)|\, d\theta \;\leq\; c\int_{-\pi}^{\pi} |(1 - z)^{-1}|\, d\theta + \int_{-\alpha}^{\alpha} |h(z)|\, |1 - z|\, d\theta.$$

We wish to find upper bounds for the integrals on the right. Now

$$(1 - z)^{-1/2} = \sum_{n=0}^{\infty} u_n z^n,$$

where $u_n = O(n^{-1/2})$. Hence

$$\int_{-\pi}^{\pi} |(1 - z)^{-1}|\, d\theta = \int_{-\pi}^{\pi} \left|\sum_{n=0}^{\infty} u_n\, z^n\right|^2 d\theta$$

$$= \int_{-\pi}^{\pi} \left|\sum_{n=0}^{\infty} u_n r^n(\cos n\theta + i \sin n\theta)\right|^2 d\theta$$

$$= \sum_{n,\ell=0}^{\infty} u_n u_\ell\, r^{n+\ell} \int_{-\pi}^{\pi} \cos(n - \ell)\theta\, d\theta = 2\pi \sum_{n=0}^{\infty} u_n^2\, r^{2n}.$$

It follows that

$$\int_{-\pi}^{\pi} |(1 - z)^{-1}|\, d\theta \leq k_1 \sum_{n=1}^{\infty} \frac{r^{2n}}{n}.$$

Now

$$\log\frac{1}{1 - r} - \sum_{n=1}^{\infty} \frac{r^{2n}}{n} = \log\frac{1}{1 - r} - \log\frac{1}{1 - r^2} = \log(1+r) > 0.$$

Hence

$$(3.1.12) \qquad \int_{-\pi}^{\pi} |(1 - z)^{-1}|\, d\theta < k_1 \log\frac{1}{1 - r}.$$

Now

$$|1 - z| = |1 - re^{i\theta}| = (1 - 2r\cos\theta + r^2)^{1/2}$$

$$\leq \{1 - 2r(1 - \theta^2/2) + r^2\}^{1/2} \leq (1 - r) + \sqrt{r}\,|\theta|$$

$$\leq \alpha(1 + \sqrt{r}) \leq k_2\alpha.$$

Hence

$$\int_{-\alpha}^{\alpha} |1 - z|\,|h(z)|\,d\theta \leq k_2\alpha \int_{-\alpha}^{\alpha} |h(z)|\,d\theta.$$

By Schwarz' inequality for integrals,

$$\int_{-\alpha}^{\alpha} |h(z)|\,d\theta \leq \left(\int_{-\alpha}^{\alpha} d\theta\right)^{1/2} \left(\int_{-\alpha}^{\alpha} |h(z)|^2\,d\theta\right)^{1/2}.$$

Hence

$$(3.1.13) \quad \int_{-\alpha}^{\alpha} |1 - z|\,|h(z)|\,d\theta \leq k_2\alpha^{3/2} \left(\int_{-\pi}^{\pi} |h(z)|^2\,d\theta\right)^{1/2}$$

where we have again used the fact that $\alpha < \pi$ in changing the limits of integration. It is easy to show that

$$(3.1.14) \qquad \int_{-\pi}^{\pi} |h(z)|^2\,d\theta = 2\pi \sum_{n=0}^{\infty} v_n^2\, r^{2n}.$$

We may write

$$\sum_{n=0}^{\infty} v_n^2\, r^{2n} = \sum_{n \leq (1-r)^{-1/2}} v_n^2\, r^{2n} + \sum_{n > (1-r)^{-1/2}} v_n^2\, r^{2n}.$$

Since $v_n = o(n^{1/4}/\sqrt{\log n})$, we have, for $n \leq (1 - r)^{-1/2}$, $v_n^2 < k_3 n^{1/2}$, and for $n > (1 - r)^{-1/2}$, $v_n^2 < \eta(r)n^{1/2}/\log n$, where $\eta(r)$ can be made smaller than any preassigned positive number by taking r sufficiently close to 1. Hence

$$\sum_{n=0}^{\infty} v_n^2 r^{2n} < k_3 \sum_{n \leq (1-r)^{-1/2}} n^{1/2} r^{2n} \tag{3.1.15}$$

$$+ \eta(r) \sum_{n > (1-r)^{-1/2}} n^{1/2} r^{2n}/\log n .$$

The first sum on the right in (3.1.15) has $[(1 - r)^{-1/2}]$ terms, each of which does not exceed $(1 - r)^{-1/4}$. Also it is easy to verify that if $n > (1 - r)^{-1/2}$, $1/\log n < 2 \log^{-1}(1/(1 - r))$. Hence

$$\sum_{n=0}^{\infty} v_n^2 r^{2n} < k_3(1 - r)^{-3/4}$$

$$+ 2\eta(r) \log^{-1}\left(\frac{1}{1 - r}\right) \sum_{n > (1-r)^{-1/2}} n^{1/2} r^{2n} . \tag{3.1.16}$$

Now

$$\sum_{n > (1-r)^{-1/2}} n^{1/2} r^{2n} < \sum_{n=0}^{\infty} n^{1/2} r^{2n} < \frac{k_4}{2}(1 - r^2)^{-3/2}$$

$$< \frac{k_4}{2}(1 - r)^{-3/2}$$

where we have used the fact that

$$(1 - r^2)^{-3/2} = \sum_{n=0}^{\infty} \gamma_n r^{2n} , \quad \gamma_n \sim n^{1/2} .$$

This, with (3.1.16), gives

$$(3.1.17) \quad \sum_{n=0}^{\infty} v_n^2 r^{2n} < k_3(1-r)^{-3/4} + k_4\,\eta(r)\,(1-r)^{-3/2}\log^{-1}\left(\frac{1}{1-r}\right)$$

$$= (1-r)^{-3/2}\log^{-1}\left(\frac{1}{1-r}\right)\{k_4\,\eta(r) - k_3(1-r)^{3/4}\log(1-r)\}.$$

Let $\epsilon > 0$ be given. Then for $r > r_1(\epsilon)$, $\eta(r) < \frac{\epsilon^2}{2}$ and for $r > r_2(\epsilon)$, $|k_3(1-r)^{3/4}\log(1-r)| < \frac{\epsilon^2}{2}k_4$. Hence, for $r > \mathrm{MAX}(r_1(\epsilon), r_2(\epsilon))$,

$$(3.1.18) \quad \sum_{n=0}^{\infty} v_n^2 r^{2n} < k_4\,\epsilon^2(1-r)^{-3/2}\log^{-1}\left(\frac{1}{1-r}\right).$$

From (3.1.13), (3.1.14) and (3.1.18) we get

$$(3.1.19) \quad \int_{-\alpha}^{\alpha} |1-z|\,|h(z)|\,d\theta < k_5\,\alpha^{3/2}\,\epsilon\,(1-r)^{-3/4}\log^{-1/2}\left(\frac{1}{1-r}\right).$$

From (3.1.11), (3.1.12) and (3.1.19) we get

$$(3.1.20) \quad \int_{-\alpha}^{\alpha} |H(z)|\,d\theta < k_6\log\left(\frac{1}{1-r}\right) + k_5\,\alpha^{3/2}\,\epsilon(1-r)^{-3/4}\log^{-1/2}\left(\frac{1}{1-r}\right).$$

We next obtain a lower bound for the integral $\int_{-\alpha}^{\alpha} |H(z)|\,d\theta$.

Consider first the case where $H(z) = g^2(z)$. In Lemma 3.1.1, take $\varphi(z) = g(z) = \sum_{k=1}^{\infty} z^{a_k}$. Then

$$\int_{-\alpha}^{\alpha} |g^2(z)|\,d\theta \geq \frac{\alpha}{3\pi}\int_{-\pi}^{\pi} |g^2(z)|\,d\theta .$$

It is readily shown that

$$\int_{-\pi}^{\pi} |g^2(z)|\,d\theta = 2\pi\sum_{k=1}^{\infty} r^{2a_k} = 2\pi\,g(r^2) .$$

Hence

$$\int_{-\alpha}^{\alpha} |g^2(z)|\, d\theta \;\geq\; \frac{2\alpha}{3}\; g(r^2) \tag{3.1.21}$$

From (3.1.10), with $H(z) = g^2(z)$, we have

$$(1 - z)^{-1}\, g^2(z) \;=\; c\, z(1 - z)^{-2} + h(z).$$

Hence

$$g^2(r^2) \;=\; cr^2(1 - r^2)^{-1} + (1 - r^2) \sum_{n=0}^{\infty} v_n\, r^{2n}\,.$$

Now $|v_n| > kn^{1/4}$ for every constant k and sufficiently large n is incompatible with $v_n = o(n^{1/4}/\sqrt{\log n})$. Hence $v_n = O(n^{1/4})$. This yields

$$\begin{aligned} g^2(r^2) &= cr^2(1 - r^2)^{-1} + (1 - r^2)\, O \sum_{n=0}^{\infty} n^{1/4}\, r^{2n} \\ &= cr^2(1 - r^2)^{-1} + (1 - r^2)\, O\,(1 - r^2)^{-5/4} \\ &= cr^2(1 - r^2)^{-1} + O\,(1 - r)^{-1/4}, \end{aligned} \tag{3.1.22}$$

where we have used

$$(1 - r^2)^{-5/4} = \sum_{n=0}^{\infty} \gamma_n\, r^{2n}\,, \quad \gamma_n \sim n^{1/4}.$$

For $1/2 < r < 1$, $r^2(1 - r^2)^{-1} > \frac{1}{8}(1 - r)^{-1}$. This, with (3.1.22), gives

$$g^2(r^2) \;>\; k_7(1 - r)^{-1}\,. \tag{3.1.23}$$

Combining (3.1.21) and (3.1.23) we get

$$\int_{-\alpha}^{\alpha} |g^2(z)|\, d\theta \;>\; k_8\, \alpha(1 - r)^{-1/2}\,. \tag{3.1.24}$$

We therefore have, from (3.1.20) and (3.1.24)

$$(3.1.25)\quad k_8\,\alpha(1-r)^{-1/2} < k_6 \log\left(\frac{1}{1-r}\right) + k_5\,\alpha^{3/2}\,\epsilon(1-r)^{-3/4}\log^{-1/2}\left(\frac{1}{1-r}\right).$$

Choose ϵ such that $k_8\,\epsilon^{-2/3} > k_6 + k_5$. Set $\alpha = \epsilon^{-2/3}(1-r)^{1/2}\log\left(\frac{1}{1-r}\right)$ in (3.1.25). This gives, after simplification,

$$k_8\,\epsilon^{-2/3} < k_6 + k_5 .$$

This is a contradiction. The theorem will be established for the case $H(z) = g^2(z)$ if we show that

$$1 - r < \epsilon^{-2/3}(1-r)^{1/2}\log\left(\frac{1}{1-r}\right) < \pi .$$

This inequality is equivalent to

$$\epsilon^{2/3}(1-r)^{1/2} < \log\left(\frac{1}{1-r}\right) < \frac{\pi\,\epsilon^{2/3}}{(1-r)^{1/2}}$$

which is clearly satisfied when r is sufficiently close to 1.

We consider next the cases $H(z) = \frac{1}{2}(g^2(z) + g(z^2))$ and $H(z) = \frac{1}{2}(g^2(z) - g(z^2))$, and we discuss these simultaneously. The preceding proof is valid up to equation (3.1.20), i.e. we have

$$(3.1.26)\quad \int_{-\alpha}^{\alpha} \frac{|g^2(z) \pm g(z^2)|}{2}\,d\theta < k_6 \log\left(\frac{1}{1-r}\right) + k_5\,\alpha^{3/2}\,\epsilon(1-r)^{-3/4}\log^{-1/2}\left(\frac{1}{1-r}\right).$$

A lower bound for the integral on the left must be obtained.

Now

$$(3.1.27) \qquad \int_{-\alpha}^{\alpha} \frac{|g^2(z) \pm g(z^2)|}{2}\, d\theta \ \geq\ \frac{1}{2}\int_{-\alpha}^{\alpha} |g^2(z)|\, d\theta \ -$$

$$\frac{1}{2}\int_{-\alpha}^{\alpha} |g(z^2)|\, d\theta \ \geq\ \frac{\alpha}{3}\, g(r^2) \ - \ \frac{1}{2}\int_{-\alpha}^{\alpha} |g(z^2)|\, d\theta$$

where we have used (3.1.21). By Schwarz' Lemma

$$\int_{-\alpha}^{\alpha} |g(z^2)|\, d\theta \ \leq \ \left\{ \int_{-\alpha}^{\alpha} d\theta \right\}^{1/2} \left\{ \int_{-\alpha}^{\alpha} |g(z^2)|^2\, d\theta \right\}^{1/2}$$

Now

$$\int_{-\alpha}^{\alpha} |g(z^2)|\, d\theta \ \leq \ \int_{-\pi}^{\pi} |g(z^2)|^2\, d\theta \ = \ 2\pi \sum_{k=1}^{\infty} r^{4a_k} .$$

Hence

$$(3.1.28) \qquad \int_{-\alpha}^{\alpha} |g(z^2)|\, d\theta \ \leq \ 2\sqrt{\pi\alpha}\ \ g^{1/2}(r^4) .$$

Combining (3.1.27) and (3.1.28) we get

$$(3.1.29) \qquad \int_{-\alpha}^{\alpha} \frac{|g^2(z) \pm g(z^2)|}{2}\, d\theta \ \geq \ \frac{\alpha}{3}\, g(r^2) - \sqrt{\pi\alpha}\ \ g^{1/2}(r^4).$$

We are assuming that (3.1.10) holds. Hence

$$g^2(z) \ \pm \ g(z^2) \ = \ 2cz(1 - z)^{-1} + 2(1 - z)\, h(z)$$

so that

$$
(3.1.30) \qquad
\begin{aligned}
g^2(r^2) \ &\geq \ 2cr^2(1 - r^2)^{-1} + 2(1 - r^2)\, h(r^2) - g(r^4) \\
&> \ \frac{c}{4}(1 - r)^{-1} + 2(1 - r^2)\, O \sum_{n=0}^{\infty} n^{1/4}\, r^{2n} - g(r^4) \\
&\geq \ \frac{c}{4}(1 - r)^{-1} + 2(1 - r^2)\, O\, (1 - r^2)^{-5/4} - g(r^4) \\
&\geq \ \frac{c}{4}\, (1 - r)^{-1} + O(1 - r)^{-1/4} - g(r^4) \\
&\geq \ \frac{c}{4}\, (1 - r)^{-1} - g(r^4)
\end{aligned}
$$

In order that $r(n) = cn + o(n^{1/4} \log^{-1/2} n)$ hold, we must have $a_k > Mk^2$ for some constant M and all sufficiently large k. In order to see this, let us first note that $r(n) = cn + o(n^{1/4} \log^{-1/2} n)$ implies $r(n) = cn + o(n)$. Now all sums $a_i + a_j$, where $i \leq k$ and $j \leq k$, are less than or equal to $2a_k$. If we take the first interpretation of $f(n)$, we get $r(2a_k) \geq k^2$. If we take the second interpretation, we get $r(2a_k) \geq \frac{1}{2}k(k + 1)$ while the third interpretation yields $r(2a_k) \geq \frac{1}{2}(k - 1)$. Hence $r(2a_k) \geq \frac{1}{2}k(k - 1)$ in any case. We have therefore

$$r(2a_k) = 2ca_k + o(a_k) \geq \frac{k(k - 1)}{2} . \tag{3.1.31}$$

Assume that $a_k < Mk^2$ for every constant M, i.e. assume that k^2/a_k is unbounded. Then in particular, if we chose $M = \frac{1}{6c}$, we have

$$r(2a_k) < \frac{1}{3} k^2 + o(k^2) .$$

This clearly contradicts (3.1.31). Hence there exists a constant M such that $a_k > Mk^2$ for all sufficiently large k.

We use the result just established to obtain an upper bound for $g(r^4)$. Now

$$(3.1.32)\quad g(r^4) = \sum_{k=1}^{\infty} r^{4a_k} \leq k_9 \sum_{k=1}^{\infty} r^{4Mk^2} = k_9 \sum_{k=1}^{\infty} r^{Bk^2} .$$

Let us assume that $\sum_{k=1}^{\infty} r^{Bk^2} = O(1 - r)^{-1/2}$ is false. Then, for every $M > 0$ $\sum_{k=1}^{\infty} r^{Bk^2} \geq M \sum_{k=1}^{\infty} \frac{1}{\sqrt{k}} r^k$. This may be written as $\sum_{k=1}^{\infty} \frac{r^k}{\sqrt{k}} \left\{\sqrt{k}\, r^{Bk^2-k} - M\right\} \geq 0$.

As $k \to \infty$, $\sqrt{k}\, r^{Bk^2-k} \to 0$. Hence for M sufficiently large we have a contradiction. It follows that $\sum_{k=1}^{\infty} r^{Bk^2} = O(1 - r)^{-1/2}$ and this with (3.1.32) yields

$$(3.1.33)\qquad g(r^4) < k_{10}(1 - r)^{-1/2} .$$

Combining (3.1.29), (3.1.30) and (3.1.33) we get

$$(3.1.34)\qquad \int_{-\alpha}^{\alpha} \frac{|g^2(z) \pm g(z^2)|}{2}\, d\theta > k_{11}\, \alpha(1 - r)^{-1/2} .$$

Noting the similarity between (3.1.34) and (3.1.24), we see that exactly the same argument as used in the previous case can be used here. The proof of the theorem is therefore complete.

If we take $a_k = k^2$, then it is clear that the estimation of the number of solutions of $a_i + a_j \leq n$ is equivalent to the estimation of the number of lattice points in one quadrant of a circle with radius $\sqrt{n}$. Hardy and Landau showed that in this case

$$r(n) = \frac{\pi}{4} n + o(n \log n)^{1/4})$$

cannot hold. The result of Erdös and Fuchs is almost as good as this

and has the advantage that it holds for any sequence and not just the sequence of squares. We remark in passing that for the case $a_k = k^2$, it has been conjectured that for every $\epsilon > 0$

$$r(n) = \frac{\pi}{4} n + O(n^{1/4 + \epsilon})$$

but this has not been proved.

More recently, Jurkat proved that, in the general case, the result of Erdös and Fuchs can be improved to the following:

$$r(n) \neq cn + o(n^{1/4}) .$$

His proof of this has not yet been published.

In [17] Erdös and Fuchs give a second proof that $f(n)$ cannot be constant from some point on, where $f(n)$ can have any one of the three interpretations mentioned earlier. They show that if $a_k < Ak^2$ for some constant A, then

$$\limsup_{n \to \infty} \frac{1}{n} \sum_{k=0}^{n} (f(k) - c)^2 > 0$$

for all $c \geq 0$. This clearly implies that $f(k) = m$, where m is constant, cannot hold. The proof of this result will be omitted.

The result $r(n) \neq cn + o(n^{1/4}(\log n)^{-1/2})$ implies more than the fact that $f(n)$ is not constant from some point on. We can use it to show that $f(k)$ is not periodic from some point on. Suppose $f(n)$ is periodic for $k \geq \ell$, and let the period be t. Then

$$\begin{array}{lllllll}
f(\ell) & = & f(\ell + t) & = & f(\ell + 2t) & = & \ldots \\
f(\ell + 1) & = & f(\ell + t + 1) & = & f(\ell + 2t + 1) & = & \ldots \\
\vdots & & & & & & \\
f(\ell + t - 1) & = & f(\ell + 2t - 1) & = & f(\ell + 3t - 1) & = & \ldots
\end{array}$$

Then
$$r(n) = \sum_{k=0}^{\ell} f(k) + [\frac{n - \ell}{t}] (f(\ell) + f(\ell + 1) + \ldots + f(\ell + t - 1)) + O(1)$$
$$= cn + O(1)$$

which contradicts $r(n) \neq cn + o(n^{1/4}/\sqrt{\log n})$.

BIBLIOGRAPHY

[1] Artin, E. and Scherk, P. "On the sum of two sets of integers". Annals of Math. 44 (1943), 138-142.

[2] Besicovitch, A. S. "On the density of the sum of two sequences of integers". Jour. of London Math. Soc. 10 (1935), 246-248.

[3] Brauer, A. "Über die Dichte der Summe zweier Mengen, deren eine von positiver Dichte ist". Math. Zeit. 44 (1939), 212-232.

[4] ________ "On the density of the sum of sets of positive integers, II". Annals of Math. 42 (1941), 959-988.

[5] Cheo, L. "On the density of sets of gaussian integers". American Math. Monthly, 58 (1951), 618-620.

[6] ________ "A remark on the $\alpha + \beta$ theorem". Proc. Amer. Math. Soc. 3 (1952), 175-177.

[7] Chowla, S., Mann, H. B. and Strauss, E. G. "Some applications of the Cauchy-Davenport theorem". Report of the Inst. of the Theory of Numbers, Boulder, Colorado, (1959), 325-333.

[8] Davenport, H. "On the addition of residue classes". Jour. of the London Math. Soc. 10 (1935), 30-32.

[9] Dirac, G. A. "Note on a problem in additive number theory". Jour. of the London Math. Soc. 26 (1951), 312-313.

[10] Dyson, F. J. "A theorem on the density of sets of integers". Jour. of the London Math. Soc. 20 (1945), 8-14.

[11] Erdős, P. "On the arithmetical density of the sum of two sequences one of which forms a basis for the integers". Acta Arithmetica 1 (1936), 197-200.

[12] __________ and Turán, P. "On a problem of Sidon in additive number theory and on some related problems". Jour. of London Math. Soc. 16 (1941), 212-215.

[13] __________ "On the asymptotic density of the sum of two sequences". Annals of Math. 43 (1942), 65-68.

[14] __________ "Some results in additive number theory". Proc. of the Amer. Math. Soc. 5, No. 6 (1954), 847-853.

[15] __________ "Problems and results in additive number theory". C.B.R.M. Colloque sur la Théorie des Nombres (1956).

[16] __________ "Some unsolved problems". Pub. of the Math. Inst. of Hung. Acad. of Science, 6 (1961), 221-254.

[17] __________ and Fuchs, W. H. J. "On a problem in additive number theory". Jour. of the London Math. Soc. 31 (1956), 67-73.

[18] __________ and Niven, I. "The $\alpha + \beta$ theorem and related problems". Amer. Math. Monthly, 53, No. 6 (1946), 314-317.

[19] Kasch, F. "Abschätzung der Dichte von Summenmengen". Math. Zeit. 62 (1955), 368-387.

[20] Khinchin, A. Y. "Über ein metrisches Problem der additiven Zahlentheorie". Mat. Sbornik 40 (1933), 180-189.

[21] _________ "Three pearls of number theory". Graylock Press, Rochester, N.Y. (1952), 18-36.

[22] _________ "Zur additiven Zahlentheorie". Recueil Math. de la Soc. Math., Moscou, 39 (1932), 27-34.

[23] Landau, E. "Die Goldbachsche Vermutung und der Schnirelmanneche Satz". Nachrichten Gottingen, (1930), 255-276.

[24] _________ "Über einige neure Fortschritte der additiven Zahlentheorie". Cambridge Tracts, No. 35 (1937).

[25] Lepson, B. "Certain best possible results in the theory of Schnirelmann density". Proc. of Amer. Math. Soc. 1 (1950), 592-594.

[26] Linnik, U. V. "On Erdös' theorem on the addition of numerical sequences". Rec. Math. (Mat. Sbornik) N. S. 10 (1942), 67-78.

[27] Lorentz, G. G. "On a problem in additive number theory". Proc. Amer. Math. Soc. 5, No. 5, (1954), 838-841.

[28] Mann, H. B. "A proof of the fundamental theorem on the density of sums of sets of positive integers". Annals of Math. 43 (1942), 523-527.

[29] __________ "On the number of integers in the sum of two sets of integers". Pacific Jour. of Math. 1 (1951), 249-253.

[30] Moser, L. "On the additive completion of sets of integers".

[31] __________ Oral communication.

[32] Narkiewicz, W. "Remarks on a conjecture of Hanani in additive number theory". Colloquium Mathematicum 7 (1960), 161-165.

[33] Niven, I. "On the asymptotic density of sequences". Bull. Amer. Math. Soc. 57 (1951), 420-434.

[34] __________ and Zukerman, H. S. "An introduction to the theory of numbers". John Wiley and Sons, Inc. (1960), 221-236.

[35] Ostmann, H. H. "Verfeinerte Losung der Asymptotischen Dichtenaufgabe". J. Reine Angew. Math. 187 (1950), 183-188.

[36] Report of the Institute of the Theory of Numbers. Univ. of Colorado (1959).

[37] Scherk, P. "An inequality for sets of integers". Pacific Jour. of Math. 5 (1955), 385-387.

[38] __________ "On a problem of L. Moser". Newsletter of the Can. Math. Congress, second issue, (Autumn, 1954).

[39] Schnirelmann, L. "Über additiven Eigenschaften von Zahlen". Math. Annalen 107 (1933), 649-690.

[40] Schur, I. "Über den Begriff der Dichte in der additiven Zahlentheorie". Sitzungs der preuss. Akad. der Wiss., Math. Phys. Klasse (1936), 269-297.

[41] Shapiro, H. N. "Some remarks on a theorem of Erdös concerning asymptotic density". Proc. Amer. Math. Soc. 1, No. 5 (1950), 590-592.

[42] Stalley, R. D. "A modified Schnirelmann density". Pacific Jour. of Math. 5 (1955), 119-124.

[43] Table of the Fresnel Integral to Six Decimal Places. Camb. Univ. Press (1956).